Data Protection at a Glance

What is data protection?

It is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection Acts 1988 and 2003 confer rights on individuals as well as placing responsibilities on those persons processing personal data.

To Comply with their data protection obligations data controllers must...

- obtain and process the information fairly;
- keep it only for one or more specified, explicit and lawful purposes;
- use and disclose it only in ways compatible with these purposes;
- keep it safe and secure;
- keep it accurate, complete and up-to-date;
- ensure that it is adequate, relevant and not excessive;
- retain it no longer than is necessary for the specified purpose or purposes;
- give a copy of his/her personal data to any individual, on request.

Individuals have a number of legal rights under data protection law. You can....

- expect fair treatment from organisations in the way they obtain, keep, use and share your information;
- demand to see a copy of all information about you kept by the organisation;
- stop an organisation from using your details for direct marketing;
- demand that inaccurate information about you be corrected;
- demand that any information about you be deleted, if the organisation has no valid reason to hold it;
- complain to the Data Protection Commissioner if you feel your data protection rights are being infringed;
- sue an organisation through the courts if you have suffered damage through the mishandling of information about you.

Data Protection Commissioner

Canal House, Station Road, Portarlington, Co. Laois

LoCall: 1890 252 231 Tel: +353 57 868 4800 Fax: +353 57 868 4757

e-mail: info@dataprotection.ie Web: www.dataprotection.ie

An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Eighteenth Annual Report

of the
Data Protection Commissioner
2006

Presented to each of the Houses of the Oireachtas pursuant to section 14 of the Data Protection Acts 1988 & 2003

PRN. A7/0388

Contents

Foreword

The Surveillance Society

In last year's report, I commented on the extent to which the individual's "private space" was being gradually, almost imperceptibly, eroded in this country. Some of this was due to State activity; for example, retention of telecommunications data. Often the private sector was responsible; for example, "cold-calling" people at home with unwanted marketing messages. Sometimes it was an issue of how otherwise beneficial technologies were deployed in a way that eroded privacy.

That this was a shared concern among other data protection authorities emerged forcefully at this year's international data protection conference held in London in November and hosted by our UK colleague, Richard Thomas. A thought-provoking report on "The Surveillance Society", which he had commissioned, provided the stimulus for wide-ranging discussion on how many seemingly-benign developments were adding up to a situation where the individual's "private space" was being significantly eroded. The conference acted as a "wake-up call" to all concerned as regards the quality of the democratic society we aspire to live in.

A balanced approach is essential in this area. We must recognise that a certain degree of surveillance by the State is necessary to preserve the peace and safety of the law-abiding majority. Some would argue that whether this is done by a Garda on the beat or by a clearly visible CCTV system is a matter of degree. More generally, we must also recognise the huge benefits brought by technology, some of which inevitably involve sharing of personal information.

People are different. Some guard their privacy jealously. Others cheerfully share their most intimate personal details on social networking websites such as 'Bebo' and 'My Space'. What is needed is an approach which emphasises the right of the individual to choose what personal information s/he discloses and to have some control over how it is used.

This balanced approach will influence the way in which my Office approaches the issues thrown up by the Surveillance Society in the course of 2007. We will be looking, for example, at whether CCTV systems used in commercial settings and in public spaces comply with data protection guidelines laid down respectively by my Office and by the Department of Justice, Equality and Law Reform. We will also continue to clamp-down on unwanted intrusions into 'private space' - such as through 'cold-calling' - and insist on the individual's right to access personal information that is held on them by public and private organisations.

Your right to control how, and by whom, your personal data is stored and used is important. To illustrate how important, and to highlight some of the inherent risks, we've put together on the following pages an account of a fictional, somewhat busy, day in the life of Ms. Annie Wun. The situations are dramatised but nevertheless reflect the everyday lives of the population at large.

Appreciation

Finally, as on the occasion of last year's report and even more so now, I want to take this opportunity to commend the professionalism and commitment of all the staff of my Office during what was an unusually challenging year. It was the year when an almost complete rotation of staff within the Office took place as we prepared for our decentralisation to Portarlington which was successfully completed at the start of December - one year ahead of its original schedule. Through the dedication and assistance of the former staff and the enthusiasm of the incoming staff, we have managed to ensure that the highest standards of public service which this Office has embodied over the years were more than maintained. We look forward to continuing to impact positively on the privacy landscape in 2007 and the years beyond with a renewed vigour brought about by the fresh impetus of all our staff.

Billy Hawkes
Data Protection Commissioner

Portarlington, April 2007

A Day in the Life

07:00 Annie Wun wakes up and turns on her computer to access the internet. She begins by checking the news using her account on an on-line news source. She had checked the privacy policy of the website before registering and was satisfied with the uses made of her data.

07:15 Annie searches for some personal items online. The searches together with her IP address (a unique address assigned to Annie's PC by her internet service provider (ISP)) are recorded and retained by the ISP for an unknown period of time and without a specified purpose. Searches made by Annie are also retained by the search engine and sometimes clearly used for targeted marketing purposes.

07:30 Annie phones her father to talk about a story on the news. The record of her call to her father is retained by her phone provider for a period of 3 years as required by law. It will be available to An Garda Síochána (and hopefully nobody else) should the need arise as part of any criminal investigation.

08:00 Annie leaves her house and drives to work. She passes through a toll booth using her easy travel card. Information is stored about the time her car passes through the booth and other booths along the journey each time. Again this information is retained and may be accessed for law enforcement or other purposes.

09:00 Annie reaches her workplace. CCTV cameras record her arrival as her employers are concerned about the security of the workplace. The use of CCTV was communicated to employees in advance of implementing the system and it was made clear to them that images from the system would only be used for security purposes and would be kept safe and secure.

Annie's employers were also concerned about their ability to properly track their employees in terms of time worked in the workplace so, after considering many options, they introduced a biometric thumb print clock-in system which records each employee each time they enter and leave the workplace. Annie was concerned that such a system was a bit intrusive into her personal space but most of her colleagues seemed unconcerned so she went along with it. There are no details available to Annie as to what other uses her employer might make of the information or indeed what security is in place to protect her personal data stored in the system.

09:15 Annie logs onto her email to check for any emails received. She has received a number of work related emails which require her attention and one personal email. Her employer has an email and internet usage policy in the workplace stating that some limited personal use of these facilities is permitted but that inappropriate usage is not permitted. Annie understands that this means that her employer may check her emails and internet usage from time to time or in response to a genuine suspicion of inappropriate usage. However, her employer may not check her mail or internet usage on an ongoing basis since this would intrude on her legitimate, limited personal use of these systems.

11:15 Annie uses her coffee break to check her bank balance using her bank's on-line service. Her bank knows how much use she makes of her account and has credit-profiled her based on this use for a €10,000 loan which is offered to her upon log-in. She doesn't accept.

Annie had spoken to her younger brother the previous evening and agreed to send him some additional funds. He is back-packing around Europe. Annie chooses the fund transfer option. Her bank, in common with all other major financial institutions, uses the SWIFT exchange system for such transfers. It is not made clear to Annie that details of the transfer may be accessed by the US Government as part of its efforts to combat the financing of terrorism.

13:00 Annie pops out for lunch and visits her local supermarket to pick up some things for the house as she is planning a major spring clean at the weekend. She hands in her store card to collect loyalty points as part of the purchase. Her supermarket accesses her information to monitor her buying habits and offers some suitable products in her next mail shot. She

doesn't mind as she personally doesn't care what the supermarket knows about her buying habits.

She was, of course, recorded on the shop's CCTV system as she entered and exited the shop.

13:20 Annie visits her local library to return a self help book "Male and Female Chemistry" and takes out a book on building self esteem "Love Bomb People". She uses her library card which stores her usage pattern on the local authority database.

13:45 Using her lunch-break, Annie phones the Revenue Commissioners to query her tax allowances. She gives her personal public service number (PPSN) to the person on the other end of the phone line. They use her PPSN to pull up her name and address and a complete record of her dealings with the Revenue Commissioners for the past number of years. This reveals that she is a member of a Trade Union (a fact that her employer is unaware of), pays her refuse charges and claimed a substantial amount in medical expenses the previous year.

16:00 Annie has to leave work early today to attend hospital for an appointment with her specialist. Annie still suffers from pain from an accidental shotgun wound in her leg suffered in an accident while on her family farm 3 years ago. Upon arrival, she gives her details. Her full medical file is with her specialist. This is not a concern as she wishes this to be the case. She is also aware that her full medical history is entered on an electronic system in the hospital. She does not mind this either but assumes that her records are only accessed by those persons who need her information to treat her.

18:00 Annie arrives home. She picks up her post which arrived after she left the house in the morning. Her credit card company is offering her another loan and has increased the credit limit on her card (without her asking) based on their analysis of her usage. She has also received direct marketing from a company with which she had no previous dealings offering her services for the property for which she has just made a planning application. She is very surprised at this as the local authority had not informed her that her personal details would be made public as part of the planning process. She has also received an unwanted text message offering her similar services. She is also very surprised by this but remembers that her local authority had asked her for her mobile phone number as a means of contacting her.

19:00 Having eaten dinner, Annie logs onto the internet again and books a flight to New York (she will in fact have minor plastic surgery undertaken). In doing so, a large amount of her personal details, which she was required to make available to book the flight, will be made available to the US authorities, in advance of her travelling, as part of its security procedures. Using this information, an assessment will be made as to whether she poses a threat to US security. The airline, through on-screen information, had provided some details of this but Annie does not normally read all such optional information, so is not aware of this.

20:00 Annie receives a call on her mobile phone. She doesn't recognise the number but answers it in any case. Upon hearing her name the person hangs up and Annie thinks nothing more of it. Unknown to Annie, the person who had phoned her number by accident is suspected of criminal activity by An Garda Síochána. They will shortly make a formal request under the provisions of the Criminal Justice Act 2005 for all records of phone activity by that person. This will highlight that Annie's number was phoned. As a result, An Garda Síochána will also request all details of her mobile phone usage for the past 3 months to ascertain whether she is relevant to their inquiries. This will ultimately reveal that she is not but only after all her mobile phone usage - including her location when she made and received calls - is thoroughly examined.

Annie finishes her day by watching Big Brother on television. Her personal data is not made available to anybody else for the rest of the day.

Surveillance Society?

Well, why would law-abiding Annie Wun have anything to worry about? Her daily life has been made easier by the use of modern technology and she has willingly shared her personal information to get these benefits. Then again, perhaps she should worry. What if the information retained about her were pulled together in one place? The profile which emerges, and the conclusions that could be drawn from it, might give her an unpleasant surprise. Step forward Annie Wun, terrorist suspect?

ANNIE WUN:

Internet News Search:	Articles of Interest include "London Terrorists Charged" (internet records).
Web searches:	Plastic surgery.
Fund Transfer:	Made out to a male in Hamburg.
Medical records:	Operated on for gunshot wound.
Criminal records/offences committed:	Yes. (Two speeding fines)
Local Authority library files:	A word search threw up two hits - "chemistry" and "bomb".
Phone records:	Call received from known criminal.
Shopping habits:	Large variety of hazardous cleaning materials purchased.
Holiday plans:	Travelling on a flight to New York next week.

Part 1 - Activities in 2006

Introduction

2006 was a year of intense activity for the Office. As we prepared for, and carried out, our decentralisation to Portarlington, we were engaged in a number of high-profile campaigns designed to raise awareness about data protection rights and obligations. A number of initiatives were undertaken to further improve our customer services, ranging from ongoing improvements to the service we provide via our website to the creation of a dedicated customer helpdesk to deal with the ever-increasing number of queries. In all of this my Office retained its capacity to react to important issues of public concern as they arose. These varied from individual complaints about breaches of data protection rights to inappropriate use of CCTV cameras and allegations of unauthorised sharing of personal information by mortgage brokers and estate agents.

Customer Service

DECENTRALISATION

The Tánaiste and Minister for Justice, Equality & Law Reform, Mr. Michael McDowell, T.D., officially opened our newly decentralised offices in Portarlington, Co. Laois on Monday 11th December. Minister of State at the Office of Public Works, Mr. Tom Parlon, T.D. also attended this event which marked the culmination of a great deal of effort to ensure that our decentralisation project was carried out with the minimum disruption to our customer service commitments. In the event, our move to Portarlington took place one year ahead of schedule.

As an Office that has actually decentralised, I might just say a few words about our experiences. The first and most important point is that the move has indeed been successful for all concerned. For the staff themselves, they have replaced sometimes 4 hour total commutes in the one day with a 10-15 minute typical journey time each way. The rebalancing of work-life for all concerned is a strong positive for the Office going forward in terms of staff commitment. We remain accessible to our customer base and as with any organisation undergoing such change, the fresh impetus brought by new staff (all but one of our former staff left during the course of the year) has presented a unique opportunity to re-assess the way we carry out our functions. We have seized this opportunity and tried to ensure that we are organised to provide a high quality public service to all our customers.

We were fortunate that the professionalism and dedication of former staff members was such that they handled the process of handover with enthusiasm and commitment. We identified from the outset that appropriate and focused training would be key. This training included long periods of overlap for outgoing staff with those who were coming into the Office; return-visit workshops from former staff members; courses by academics prominent in the field of data protection; and a series of visits from experienced colleagues working in the data protection authorities of other EU countries.

The impact of training and other initiatives aimed at minimising disruption was indispensable for our continued commitment to high standards of customer service. These initiatives included a dedicated helpdesk system that was put in place at an early date to ensure that members of the public were able to access helpful, informed advice throughout the course of the year.

The success of these initiatives is apparent in the continued capacity of our Office to proactively develop our education and awareness-raising functions; to respond to data protection complaints from our customers; to continually update ourselves in the face of new challenges; and to maintain and develop the international role of the Office. The Office has also retained and perhaps even enhanced its ability to react to external events not within our direct control. This continued capacity was best demonstrated by our immediate follow-up to a series of high-profile events with data protection implications which are outlined elsewhere in this report.

THE PROVISION OF INFORMATION AND ADVICE

Customer service is at the centre of the mission, strategy and identity of the Office of the Data Protection Commissioner. Our customers include members of the public who contact the Office to seek information or to make a complaint; members of the public who are not yet aware of their rights under data protection legislation; and data controllers and those who represent or advise them seeking to ensure that their business practices are in compliance.

Our mission - to protect the individual's right to privacy by enabling people to know, and to exercise control over how their personal information is used, in accordance with the Data Protection Acts, 1988 & 2003 - commits us to providing an effective service for all these customer groups. The potentially disruptive period of our decentralisation to Portarlington posed particular challenges in regard to the fulfilment of our mission in 2006. Our website (www.dataprotection.ie) has proved to be a valuable means of keeping our customers informed of their rights and obligations and updated on ongoing developments. Recognising that this facility has quickly become our primary customer interface (it was accessed over 69,000 times from Ireland last year, with another 134,500 visits from other European countries), we are currently undertaking a review and redevelopment of the website to make it hopefully still more customer-friendly and accessible. We have already launched a new feature in the form of a registration-on-line facility to make it easier for data controllers and processors to register. Over the past year our helpdesk has responded to over 20,000 phone calls, together with over 2,000 email enquiries and a smaller number of contacts by post. These large increases are explained by a number of very effective education and awareness-raising exercises, increasing numbers of audits and inspections and a higher media profile as journalists continued to engage with the Office and with the issues at stake. The role played by the national and local media in increasing public awareness of data protection issues is particularly valuable in helping members of the public to understand and safeguard their rights.

The 34 presentations by staff of the Office to various sectors and organisations (see appendix 1) provided another excellent opportunity to raise awareness of the obligations of data controllers under the Data Protection Acts. The resulting personal interaction created a space where the data protection implications of new technologies and business approaches could be explored in detail.

Freedom of Information (FOI)

The majority of public bodies are subject to the Freedom of Information Acts as well as to the Data Protection Acts. The two legal codes largely complement and reinforce one another. They both provide for an individual's right to access her/his personal information. They also restrict the disclosure of personal information to third parties.

The FOI Central Policy Unit in the Department of Finance issued guidance to public bodies on how to deal with access requests under both codes in December. The guidance[1] provides that public bodies should take account of both codes when processing requests for access to personal information.

I very much welcome this development. The guidance should ensure that access requests are viewed from the viewpoint of the individual, who should be afforded the rights provided in both codes.

The guidance was drawn up in consultation with this Office and the Office of the Information Commissioner. It is yet another example of the close cooperation between us.

Business Plan Report

Our Business Plan in 2006 was prepared with the challenges of decentralisation to Portarlington very much in mind. Against such a background, the

[1] The Guidance Notice referred to is available at www.foi.gov.ie under "Central Policy Unit Notices".

continued provision of a professional and efficient service to our customers was naturally the cornerstone of our Plan. I am pleased to confirm that, through the comprehensive training programme outlined above and thanks to the efforts of former and new staff, the targets outlined in that plan were substantively met and, as will be clear from the remainder of the Report, exceeded in many instances. Overall, we continue to strive to meet our goal of performing our independent functions in a transparent, accountable and efficient manner.

Irish Language Scheme

In the spirit of quality customer service, my Office has prepared an Irish Language Scheme in accordance with the Official Languages Act 2003. In adopting the scheme, the Office commits itself to ensuring better availability and a higher standard of public service through Irish. We published a notice in July 2006 inviting submissions from interested parties in relation to the preparation of the scheme. We are very grateful to those who put their time and effort into the five submissions we received. The scheme, which came into effect on 1st April 2007, was developed with these submissions in mind.

At present my Office provides a number of services bilingually. Our main corporate publications - the Annual Report and the Customer Service Action Plan - are available in both Irish and English. We ensure that members of the public who wish to conduct their business through Irish are facilitated and we respond in Irish to correspondence received in Irish. We also aim to respond in Irish to telephone callers who wish to speak in Irish; we do this immediately where possible or we offer to have the call returned promptly by a member of staff who can deal with queries in Irish. Our signage and our office stationary are in both languages. Our website is navigable in Irish.

Our commitments under our Irish Language Scheme are focused on improving the range of written and electronic means of communication available bilingually and on developing Irish language competency amongst staff to facilitate improvements in interpersonal Irish language service delivery.

Complaints and Investigations

Under the Data Protection Acts, 1988 & 2003, I may launch an investigation into the possible contravention of the Acts when an individual complains to me that their data protection rights have been infringed in any way, or when I am of the opinion that there may be a contravention. When a complaint is received I am required by section 10 of the Acts to investigate it and to try to arrange an amicable resolution. Failing that, I am required to issue a decision in relation to it. As in previous years, my Office managed to resolve the greater proportion of complaints without it being necessary for me to issue a formal decision under section 10.

An effective complaints and investigations function is of central importance to the role of my Office. Addressing alleged contraventions of the Acts in a proactive manner allows individuals to see that the upholding of their data protection rights is a responsibility that is taken seriously by my Office. Perhaps more importantly it demonstrates to data controllers that such issues are taken seriously and that they need appropriate structures to ensure that they meet their responsibilities and that breaches, where they occur, are the exception rather than the rule. Where data controllers do not respond appropriately to my Office, I do not hesitate, where necessary, to use the very strong powers which I am given to require data controllers to desist from practices that breach the Acts. In addition, where I find that there has been a breach of the Acts, individuals may use my decision to support a claim for damages in the courts under section 7 of the Acts.

The number of new complaints received during the year was 658 (compared to 300 in 2005). Figure 1 shows complaints received, concluded and outstanding for 2006 and 2005. The biggest factor in this increase was the significant increase in the number of complaints dealt with under the Privacy in Electronic Communications Regulation (S.I. No. 535 of 2003). 264 such complaints were dealt with in 2006 compared with 66 in 2005.

Figure 1 Complaints Received, Concluded and Outstanding

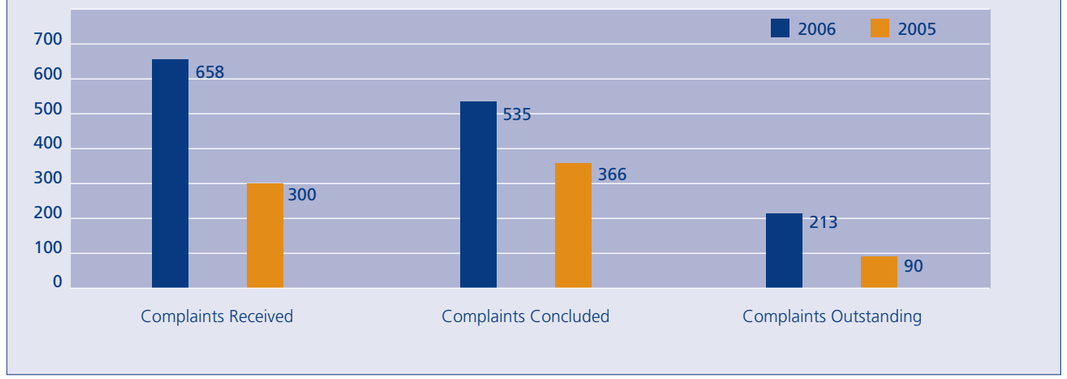


Figure 2 illustrates the breakdown of complaints by data protection issue. The large number of complaints received under SI535 is also apparent from this breakdown. As well as an increase in marketing activity in this sector, this increase reflects a much greater level of public awareness of the right not to receive unsolicited marketing communications in this manner. The next most common area of complaints concerned the exercise of the right of access to one's own personal data under section 4 of the Act. The details of some of these complaints cases are summarized in the Case Studies section of this Report.

Figure 2 Breakdown of Complaint by Data Protection issue

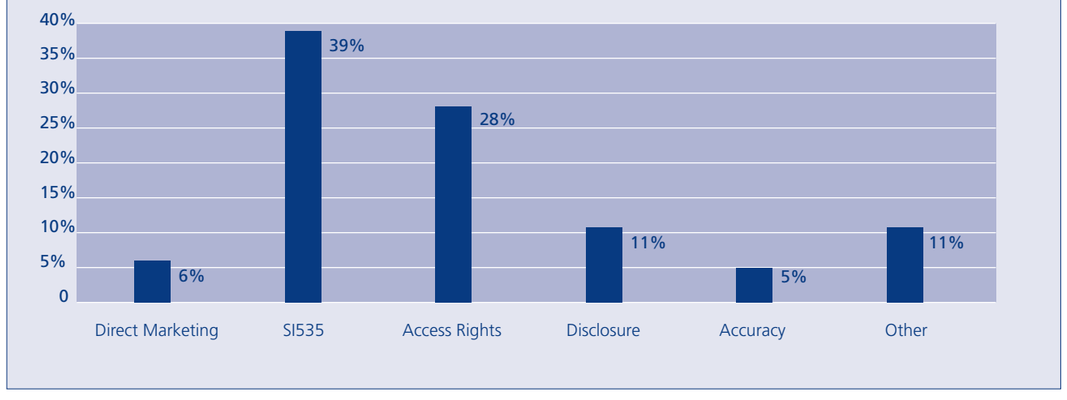
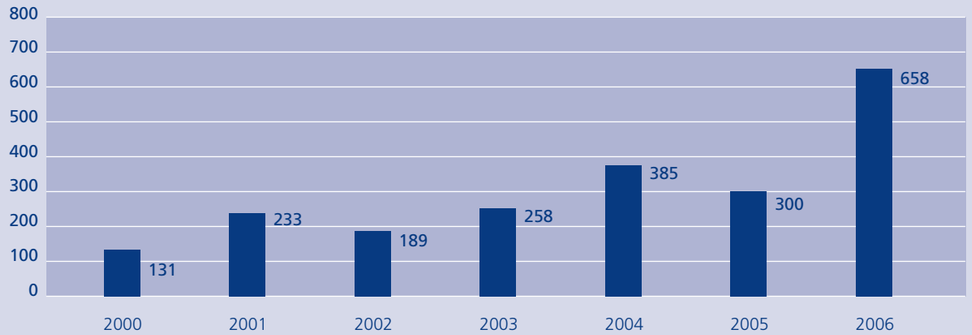


Figure 3 Complaints received since 2000



INCREASED USE OF ENFORCEMENT POWERS

The right of access to personal data is a fundamental right that is enshrined in data protection legislation. I have the power to take immediate action to vindicate this fundamental right of a data subject. In response to the increase in the number of complaints received in relation to such requests, following a review, we have radically altered our approach to resolving these complaints to better serve the interests of data subjects. **The emphasis now is on enforcement.** Data controllers who fail to inform the data subject of the reasons for refusing an access request contravene Section 4(7) of the Acts. Under the new procedures, data controllers who appear to be breaking the law in this way are given ten days from the start of my investigation to inform the data subject in writing (and to copy the correspondence to my Office) of the provisions of the Acts which s/he is relying on to withhold the personal data or, if he/she has no provisions to rely on, to comply with the access request immediately.

The data controller is informed that if, within the ten days, the access request is not complied with, I will commence enforcement proceedings fourteen days from the start of my investigation. I will not take such action in the rare case where the data controller can demonstrate that access can be denied under one of the exceptions provided for in the Acts.

Failure to comply with an Enforcement Notice is an offence liable to a fine on summary conviction in the District Court of €3,000.

I am confident that the new strategy which I have put in place will help considerably to enforce the legitimate rights of data subjects who have suffered a violation of their access rights at the hands of what are usually ill-informed but sometimes deliberately evasive data controllers. Data controllers in such situations should be aware that my enforcement powers have real teeth and I will have no hesitation in applying those powers in their direction. Furthermore, in the interests of vindicating this fundamental right of data subjects, I am not in a position to tolerate efforts by such data controllers to delay my investigations through the raising of spurious legal issues.

During the course of 2007, my Office will continue to consider additional areas of our functions where swifter recourse to legally enforceable options would be the preferred course in the interests of data subjects. I emphasise again, however, that such options are not my preferred route and my Office works extremely hard to find amicable solutions to issues as they arise.

PRIVACY AND TELECOMMUNICATIONS

Under Statutory Instrument 535 European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations of 2003, I have certain responsibilities in relation to intrusions into privacy involving use of telecommunications and other electronic communications devices. These responsibilities are in many cases shared with ComReg (the Communications Regulator). Over the last year my Office continued to enjoy a close and productive working relationship with ComReg. We have worked on a number of projects together, such as adding ex-directory subscribers to the National Directory Database (NDD). We have also worked closely together on a number of investigations, mostly in the area of cold calling by telecommunications companies.

The number of complaints I have received under SI 535 increased by a remarkable 300% in the last year from 66 in 2005 to 257 in 2006. The majority of complaints we receive in this area are related to cold calling or unsolicited SMS messages. I put at least some of this increase down to the awareness efforts of ComReg and ourselves to highlight to consumers that they do have rights in this area.

Cold Calling

Cold Calling is the making of unsolicited direct marketing phone calls. A typical case is outlined in Case Study One. It is my policy to vigorously prosecute in the case of repeat offences. In cases of first time offences, the approach is to warn that continued breaches are likely to lead to prosecution. A large number of the complaints received in relation to cold calls were not upheld because:

- the data subject believed they were on the NDD list not to receive marketing calls but in fact were not, either because they had not requested same or their provider had not acted on their request to be placed there;
- the calls were market surveys or market research, which fall outside the scope of SI 535;
- there was an existing business relationship which allows for a person to be called for the marketing of the caller's own similar or related products despite being on the NDD, once they were given an opportunity to object at the time of providing their contact details (but once the person objects subsequently to the call from that entity they must not be called again by that source).

Unsolicited SMS Messages

The number of complaints in this area is growing rapidly. Indeed, I have a concern from the evidence now coming to my attention that the issues arising in this area are even more serious. Unfortunately, there may be an element of apathy setting in on the part of recipients of such unsolicited messages due to the volume of these messsages and the complexity of the language used. I will be using my full powers in the coming year to ensure that all parts of this sector fully understand their data protection obligations. As a first step, we have issued a new guidance document on sending electronic messages that can be found in Part Three of this Report. In investigating complaints regarding unsolicited SMS messages, my Office works closely with the Regulator of Premium Rate Telecommunications Services (RegTel). Our cooperation with RegTel has proved invaluable in investigating these complaints and in coming to terms with the complexities of a rapidly evolving sector. I am grateful for the assistance extended.

Albeit in lesser numbers, my Office also deals with complaints of unsolicited emails and faxes.

National Directory Database (NDD)

The NDD 'opt-out' facility was launched by my Office, ComReg and the telecommunications industry in July 2005. SI 535 of 2003 specified the NDD as the mechanism through which subscribers may record a legally enforceable preference not to receive direct marketing calls. However, it quite quickly became clear that ex-directory subscribers were unable to have their preference recorded due to an anomaly: their numbers were not historically recorded on the NDD. This led to the unacceptable position that ex-directory subscribers were being denied the legal protection offered to listed/unlisted subscribers from cold calling.

Accordingly, discussions were held between my Office, ComReg and Eircom which, as part of its universal service obligation, administers the NDD. An industry forum was also reconvened by ComReg to consider the various options put forward for giving legal protection to ex-directory subscribers.

A key difficulty in this area was a concern on the part of telecommunications companies as to their potential legal liability to an ex-directory subscriber should their details be further disclosed beyond the NDD if they went ahead and placed it there. However, as I was determined to give ex-directory subscribers the appropriate legal protection, I issued an enforcement notice to all relevant telecommunications providers stipulating that they be in a position by 30th October 2006 to supply the details of their ex-directory subscribers' numbers, and their preference not to receive cold calls, to the NDD. Directions were simultaneously issued by ComReg to the NDD and to the industry. Furthermore, all ex-directory subscribers had to be informed of the process prior to 30th October 2006. The notice had the dual effect of giving the telecommunications companies the legal protection they were seeking while giving ex-directory customers - those most concerned about their privacy - the right to reject unsolicited marketing calls.

I am glad to say that, due to the efforts of the companies and particularly of ComReg, ex-directory customers were successfully added to the NDD 'opt-out' list. In December 2006 Commissioner Mike Byrne (Chairperson of ComReg) and I launched a press campaign to inform consumers of these changes and how they can exercise their right to be included in the NDD. At 20th February 2007, 47% of all landlines in the country had been placed on the NDD 'opt-out' list.

Privacy Audits and Random Inspections

The Data Protection Amendment Act 2003 allows me to carry out privacy audits and random inspections to ensure compliance with the Acts and to identify possible breaches. Such audits are supplementary to investigations carried out in response to specific complaints. I am pleased that during 2006 my Office adopted a very proactive role in this regard, despite the challenges of decentralisation.

In the course of 2006, eight comprehensive audits were carried out. Those audited were:

Department of Social and Family Affairs

Newtel Communications Ltd.

Dell Ireland Ltd.

Eurodac[2]

Meteor Mobile Communications Ltd. (volunteered)

Garda Síochána (Europol activities)

Demographics Ireland Ltd

Revenue Commissioners (EU Customs Information System activities)

As in 2005, my inspection teams found that there is a reasonably good awareness of, and compliance with, the data protection principles in the organisations that were inspected. Recommendations were made in a number of cases. I am pleased to report that the data controllers concerned were willing to put procedures in place to ensure that they were fully compliant with their data protection responsibilities. I would like to thank all eight organisations for their cooperation. Unfortunately, in the case of one of the organisations audited, system problems developed in relation to their direct marketing efforts subsequent to the audit (see case study number 3).

I believe such privacy audits are a very valuable tool for improving compliance with data protection principles and I intend to increase the number conducted in the course of 2007 to closer to thirty or perhaps even more.

In addition to the privacy audits, my Office engaged in a number of random inspections towards the end of 2006. These inspections took place in the wake of the allegations made about the mortgage brokerage and estate agent sectors on the Prime Time Investigates TV programme of 11th December, 2006.

In relation to this particular investigation, I was pleased to be able to make a contribution, within the functions of my Office, to the public concern that arose in the immediate aftermath of that programme. I did this by sending in inspection teams using our powers to enter premises. In fact my Office entered the premises of one mortgage broker before the broadcast of the programme. The allegations initially centred on the disclosure by mortgage intermediaries to estate agents of confidential personal data such as annual income, parental financial assistance, SSIAs etc. As part of my response, I met with the main broker representative bodies on 12th December, 2006, to discuss the issues and a plan of action to improve data protection compliance in the sector. I also maintained close contact with the Financial Regulator. My Office then proceeded to carry out a number of random, on the spot inspections of mortgage brokers and estate agents throughout December. These continued during January. My findings indicated a lack of knowledge amongst mortgage intermediaries in relation to the full extent of their responsibilities under the Acts.

A key breach identified in the course of one inspection was the casual and persistent exchange of emails disclosing personal client information between a leading mortgage brokerage and an estate agent. Payment of commissions or 'introducer fees' in return for leads provided to brokers was also a central area for concern. Here, evidence of systemic privacy breaches was uncovered where the purchase loan amount and name of the buyer was passed back to introducers without the consent or knowledge of the customer. No information on this practice was flagged up front to customers on company booking forms, sales enquiry sheets or terms of business documents. As a result of my investigations, on 21st December, 2006 I issued a guidance note and a Data Controller's booklet to all 1,633 mortgage intermediaries registered with the Financial Regulator. A key message I wished to convey was the importance of using and disclosing personal client data in a way compatible with the purpose for which it was initially given. I also recommended that a mortgage broker should put in place a written agreement with the providers of leads to ensure each named lead had consented to the disclosure of their information to the broker. As a result of this mail-shot my Office received a considerable degree of feedback from mortgage intermediaries. I am pleased to observe that our ongoing engagement and interaction with the sector has lead to many positive revisions of procedures and codes in relation to customer confidentiality. It is my intention that my Office will nevertheless continue the programme of random inspections of mortgage intermediaries throughout 2007 in order to monitor progress on foot of the issue of this guidance material.

Promoting Awareness

As I indicated in my first report as Commissioner, I place a particular emphasis on the awareness raising functions which I am assigned. Indeed, increasing awareness and understanding of data protection issues amongst the public and those entities holding personal data is mutually beneficial. The more information that the public have about their data protection rights, the better choices they will be in a position to make about how their data is used. Equally, the better informed

[2] This is a system for the exchange of fingerprint data between EU Member States for assessing the appropriate member state to process a claim for refugee status from an asylum seeker.

data controllers are about their data protection responsibilities, the less likely that their handling of that information will give rise to problems and complaints to my Office. Accordingly, I am determined to ensure that promoting awareness becomes a major output from my Office.

During the year, the following education and awareness initiatives were undertaken:

- My Office organised and hosted a seminar to raise awareness and prompt discussion within the health sector of key privacy issues associated with health research.
- A newspaper advertisement was placed in all national daily and Sunday papers in November with regard to the direct marketing (Edited Register) aspect of the Electoral Register and the facility to 'opt-out'.
- As outlined above, in co-operation with ComReg, my Office devised a publicity campaign to promote the new telemarketing opt-out facility of the NDD. The campaign consisted of a national newspaper advertisement in December and a nationwide radio advertisement followed in February 2007.
- We ran a nationwide public awareness poster campaign on bus, rail and dart locations in November with special emphasis on direct marketing and unwanted phone calls.
- Continued participation in 'The Graduate Treasure Trail Quiz', an online competition for primary and secondary school students.
- We made 34 presentations to groups in the public, private and voluntary sectors.
- My Office contributed to the broadcast and print media as data protection issues arose. This is a key opportunity to promote awareness so my Office has an active policy of making ourselves available to the media when requested to do so.

A 2005 awareness survey found that 18 - 24 year olds display some of the lowest levels of awareness and knowledge of personal privacy issues and they regard such issues as having a low level of importance. In response to this finding I have decided to specifically target the 12-24 year old cohort. To this end I will draw upon opinions and issues expressed by teenagers and young adults, particularly in terms of their personal privacy online. Of chief concern to me is the question of how teenagers and young adults rate the importance of privacy. Do they know how much information others have about them? Do they know they have rights when it comes to text messages, prize competitions, CCTV, and personal data stored on the internet?

Accordingly, in the coming year, my Office will conduct research, consult with this age group and issue new multi-media guidance material on data protection and on-line privacy through websites, schools, colleges and other media that is actually used by the target age group. In particular, I wish to engage with local schools and pupils drawn from Portarlington and the surrounding district. I also intend to work closely with the Internet Advisory Board (IAB), on which my Office is represented, and with the National Centre for Technology in Education (NCTE) in relation to any online privacy issues or initiatives targeted at teenagers or their parents.

Health Issues

Physical and mental health information is considered sensitive personal information under the Data Protection Acts and therefore warrants special attention from this Office. During the year, the area of health was a priority area of policy development for my Office given the nature and increasing volume of queries received.

Data protection in the health field is essentially about respecting the confidentiality of information about patients. It complements the strong ethical obligations imposed on health professionals in relation to their patients. The key principle for me when providing advice in this area is that respect should be maintained for a patient's reasonable expectation that their health information will be kept confidential. It should not be disclosed without their consent other than to those directly involved in patient care and related activity.

SEMINAR

In response to the number of queries received in the health field, particularly in relation to research and clinical audit matters, my Office organised and hosted a seminar to raise awareness and prompt discussion within the health sector of key privacy issues associated with health research. The seminar, which was entitled ***'Promoting Health Research & Protecting Patient Rights',*** took place in Killenard, Co. Laois on 29th November 2006.

The seminar brought together over 90 delegates drawn from across the health and research spectrum (North and South). Topics covered included the legal and ethical framework under which health professionals operate, the boundaries of patient consent, the provision of necessary information to patients, and the public good justification for research on patient identifiable information.

Opening the seminar, I expressed the hope that the discussion would provide a certain degree of clarity regarding the basis on which research and clinical audit in the health sector could be carried out within the current legal framework. A key objective for the seminar was to attempt to bring about a consensus position on how to achieve balance between a patient's right to privacy and the public interest in research taking place in some instances on identifiable personal data. I signalled my intention on foot of the seminar to issue a set of guidelines to assist health professionals in accessing or seeking to access confidential patient data for research and audit purposes. The guidelines are currently being compiled and will be advanced in consultation with key bodies. In the meantime, the presentations made on the day are available to view on www.dataprotection.ie. The draft guidelines will also be placed on the website when ready.

NATIONAL HOSPITALS OFFICE (NHO) - MEDICAL RECORDS POLICY

I also want to welcome the initiative of the National Hospitals Office Medical Records Steering Committee which has developed a comprehensive, draft NHO Medical Records and Retention Policy which was circulated for comments at the end of the year. Although still in the consultation phase, I look forward to its implementation during 2007.

Solution-oriented approach

One of the difficult areas of data protection involves managing public perceptions of our role. Sometimes we are perceived as a champion of the citizen's right to privacy. At other times, even in relation to the same issue, we are seen as blocking the sharing of information and thereby reducing the efficiency of public services. I accept it as an inevitable hazard of the job in protecting the individual's right to privacy that data protection will sometimes be portrayed as a problem. However, I am strongly of the view that this need not necessarily be the case. If my Office is approached early enough in the development of a policy or of a new data collection system, we can be part of a solution rather than a problem.

BREACH NOTIFICATION

A positive trend I have noted in the past year is a developing practice, especially in the financial sector, of notifying my Office when there has been an unintended breach of the Acts. This applies particularly where customer information has been inadvertently disclosed to others. I welcome this approach. I expect that, in most cases, such a notification will be accompanied by an immediate apology to the affected data subjects. A data controller that accepts

responsibility in this fashion is, in my opinion, acting in the spirit of the Acts. Such a data controller is also, in my opinion, less likely to have to deal with individual complaints to my Office about the breach in question.

GOVERNMENT

The EU Data Protection Directive obliges each Member State government to consult with its national supervisory authority - the Data Protection Commissioner in Ireland - when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. I am glad to say that most government departments and agencies consult my Office when developing proposals with data protection implications. I would like to thank those that did so in the course of the year. Such consultation enables this Office to work with agencies to develop privacy-friendly solutions to issues, thus avoiding subsequent difficulties with enacted legislation.

Health (Repayment Scheme) Act 2006

One such example was consultation which took place between my Office and the Department of Health and Children and the HSE in relation to the provisions in the Bill for the above Scheme relating to the access to, and processing of, personal data for the purposes of making repayments under the Scheme. While the consultation took place a little later in the drafting process than may have been optimum, both the Department of Health & Children and the HSE demonstrated a ready willingness to take account of my views in the enacted legislation. The essential issue was that the Bill as drafted contained a complete "carve out" (as I term it) from the requirements of the Data Protection Acts in relation to any of the processing of personal data that was necessary to make repayments. This approach had been proposed for reasons of efficiency as identified by the Department. In putting forward my reservations about such an approach, I was of course conscious of the strong public opinion that the Scheme should be operational as soon as possible. Accordingly I was aware that only too easily I might find myself isolated in a public debate if I opposed the proposed "carve out" too strongly. Nevertheless, in such instances I feel that I have an obligation to represent people without a voice, which in this instance were those people in nursing homes who would not be making an application under the Scheme yet whose data it was intended to access for reasons of efficiency. Equally, I was concerned that those persons making applications for repayments should continue to have rights in relation to their data supplied for the purposes of seeking a repayment. A carve out from data protection requirements of the nature initially proposed is never, in my view, an optimal outcome as the basic rights granted to a person under data protection legislation should generally apply regardless of the circumstances.

I am glad that it proved possible to meet the concerns of the Department that the Scheme be allowed to operate as efficiently as possible to ensure that those persons affected would be repaid as soon as possible. At the same time, the solution adopted met my concerns that data protection should not be set aside. The Health (Repayment Scheme) Act required that a code of practice be prepared by the HSE and Scheme Administrator, in consultation with me, dealing with the processing of personal data. This was done immediately after the enactment of the Act and is available at www.repay.ie. I would like to commend the approach of the HSE and the Scheme Administrator for engaging so positively with my Office on the Code. The Code agreed will serve as a model for other draft codes currently under discussion with other sectors.

Identity Management in the Public Service

The Department of Finance have been charged by the Government to develop a statutorily-based system of identity management for the public service which takes full account of the individual right to privacy. I very much welcome this approach. Over the years, this Office has highlighted the need to ensure that delivery of more efficient public services to the individual takes full account of the individual's need for privacy. The Office has maintained close contact with the Department of Finance to assist it with the privacy aspects of this work.

Pending the development of a comprehensive approach, the Office provided guidance to various public bodies on how service delivery could be improved without compromising privacy.

Postal Codes Discussions

In May 2005, the Minister for Communications, Marine and Natural Resources announced that a system of postcodes would be introduced in Ireland. The Minister subsequently appointed a National Postcode Project Management Board.

In the course of the year, I made a presentation to the Project Management Board on the data protection aspects of postcodes. I subsequently provided written advice designed to help the Board to arrive at a set of proposals which would meet the public good objectives of the postcodes project without giving rise to privacy/data protection issues.

Privacy Bill

In July, the Government presented a Privacy Bill to the Oireachtas (Parliament). It simultaneously presented a Defamation Bill. The Privacy Bill provides for a new tort (civil offence) in Irish law of violation of privacy. Privacy is not defined as such but a person's entitlement to privacy is described as that which might be reasonable in all the circumstances having regard to the rights of others and to public order, public morality and the common good. The Bill provides in general that there shall be a violation of privacy where:

1. a person subjects another person to surveillance;
2. a person discloses information obtained from such surveillance;
3. there is unauthorised use of the name, voice or likeness of an individual for commercial purpose;
4. letters, diaries, medical records or other documents concerning an individual or information obtained therefrom are disclosed;
5. a person is subjected to harassment.

Various exceptions and defences are provided for in the Bill - including a defence of fair and reasonable newsgathering done in good faith on an issue of public importance. A range of judicial remedies is also provided for.

The Bill can be seen as underpinning the rights contained in the Data Protection Acts. The focus in the Data Protection Acts is on encouraging compliance rather than on punitive enforcement. It will be helpful to have a clear course of judicial action and remedy spelled out in law where there has been an invasion of privacy, complementing the existing tort provided for in Section 7 of the Data Protection Acts.

The **Defamation Bill** introduces the defence of "fair and reasonable publication on a matter of public importance" in an action for defamation. This addresses concerns that the present law on defamation unduly inhibits reporting by the media on issues of public concern. It also provides for the recognition of a Press Council that would adopt a Code of Standards and appoint a Press Ombudsman. The Ombudsman would investigate complaints of media abuse, including invasion of privacy.

Section 22A of the Data Protection Acts provides a significant degree of exemption for the media from the obligations otherwise imposed on data controllers under the Act. Nevertheless, as reported elsewhere in this Report, I decided on two occasions during the course of 2006 that newspapers acted in breach of the Acts. It will be important for the Office to develop a good working relationship with the new Press Council and Ombudsman.

Both Bills were before the Oireachtas at the end of the year.

Passports Bill

During the course of the year, the Department of Foreign Affairs engaged in ongoing consultation with my Office in relation to the draft text of the above Bill which was published on 5th April 2007. The consultation centred around the inclusion of biometric data in passports and, crucially, the basis on which information supplied by a citizen for the purpose of receiving a passport can be made available for law enforcement purposes. This reflects a basic principle of data protection that personal information given by a person for one purpose should not in ordinary circumstances be used for another purpose. The prevention or detection of a crime would be the most common basis for the set aside of this principle but, even in these circumstances, it is my firm view that the bar needs to be set sufficiently high to ensure that information of this kind is not passing freely from one authority to another. This ultimately benefits Government also as a perception on the part of citizens that their information is moving freely through Government systems would discourage the making available of that very information in the first place.

Electoral Register

An issue that attracted significant media coverage in the latter part of the year was the provision of lists of persons who were on the 'old' electoral register and not on the 'new' draft register. In our advisory role, we were approached on this issue by South Dublin County Council and after a number of contacts issued the following advice:

"There is no Data Protection difficulty with an elected representative:

- pursuing queries in relation to the status of individual persons on the electoral register if doing it on their behalf and thereby the consent of the person in question will legitimise the making available of the information;
- equally there is no problem with an elected representative pursuing queries in relation to blocks of houses in a particular area that are no longer on the register as this is aggregate data and there is no personal data involved.

We also see no difficulty with supplying an electronic copy of the draft Register as is and the previous (current!) Register to the elected representative for electoral purposes. As you (South Dublin County Council) have explained you had already done this as this is standard practice. This would be as opposed to actually processing the two Registers themselves and producing an extract of names that are no longer on the draft Register as this could give rise to Data Protection implications."

A misunderstanding that arose at the time was that I had made a "decision" on this issue. I did not. The interpretation of legislation, including the Data Protection Acts, is a matter for our Courts. The only occasion when I am required to make a decision is when I receive a complaint of an alleged breach of the Acts. In such a case, where I cannot achieve an amicable settlement (which we try hard to do as outlined elsewhere in this Report), I am obliged by the Acts to make a decision on whether or not there has been a breach of the Acts.

The advice which was given was of a type that is given on a regular basis to assist public and private bodies on how to conduct their business in a way that respects the privacy of individuals. It is not definitive nor does it have a legal standing and the person or body in receipt of that advice is free to agree or disagree with it.

Our approach was to facilitate the national drive to produce an accurate register of electors. I also fully appreciated the duty on elected representatives to hold public bodies to account in relation to how they discharge their functions - in this case, the updating of the electoral register. The advice we gave was designed to facilitate elected representatives in carrying out their duties without cutting across the individual's right to privacy.

Our concern related to those individuals who deliberately choose not to be included in the Register. We believed that their choice must be respected. The issue for local authorities, as we saw it, was whether the provision of lists of individuals who are not on the revised draft register could lead to complaints from some of these individuals to this Office that such processing of personal data breached the Data Protection Acts - this on the grounds that the local authority no longer had a basis for holding such information or disclosing it to others. If I had received such a complaint, I would have been obliged to make a decision on it - a decision which, in the circumstances, I foresaw as being difficult.

With all the above in mind, I suggested that a legislative basis be found for the provision of omission lists to elected representatives if there was a consensus that this should be done. My view was that the passage of such a provision would involve the Oireachtas making a decision that the public interest in an accurate Register should override the potential impact on the individual's data protection rights. Omission lists were provided for in an enabling provision in the Electoral (Amendment) Act 2006. The Act also extended the period during which individuals could check their details on the draft electoral register.

What is the difference between the Full Electoral Register and the Edited Electoral Register?

Since 2004, registration authorities are required to publish two versions of the Electoral Register - the 'Full' Register and the 'Edited' Register.

- The 'Full Register' lists everyone who is entitled to vote and can only be used for an electoral or other statutory purpose.
- The 'Edited Register' contains the **names and addresses** of persons whose details can be used for a purpose other than an electoral or other statutory purpose, e.g. for direct marketing use by a commercial or other organisation.

Edited Electoral Register

My Office had detailed consultations with the Department of the Environment, Heritage & Local Government on the question of how best to ensure that citizens were made aware of their right to 'opt-out' from inclusion on the edited electoral register. I was concerned that, in the effort to secure an increase in the accuracy of the register, voters would not fully understand or be aware of their right to 'opt-out' of the edited electoral register and thereby not have their details made available to direct marketers. This was a valid concern as my Office received a significant number of complaints over the past year (39) from persons who have received direct marketing material that they have not consented to receive. In the event, after the period for the insertion of names or amendment of details on the new register had closed, the number on the edited register increased to 7.05% which thankfully was not the extent which I had feared. I attribute this positive privacy outcome to several awareness raising activities, namely a circular issued by the Department of the Environment, Heritage & Local Government to all local authorities, the publication of updated guidance material on our website, and finally, a national newspaper advertising campaign that my Office conducted in early November. In light of this experience, I hope that consideration will be given when the Register is next being updated to return to the situation where entry on the edited register is by means of an opt-in rather than an opt-out.

INDUSTRY

We have also had many examples in the past year of the business sector coming to my Office for our views at the business planning stage of a proposal.

I can discern a clear pattern amongst industry to try to ensure that their applications and systems are privacy compliant and the sector, particularly in the emerging technologies area, has been constructively engaging with data protection authorities in this regard. Major

leaders in the area such as Google and Intel have sought to cooperate with my Office in this manner.

I welcome industry coming to my Office looking for a steer on issues and, although it can place pressure on the resources of the Office, it is more than recompensed in the long term. It is my firm view that building privacy in from the design stage, rather than trying to insert it when it can be too late, results in a reduction in complaints to my Office by the public that their privacy has been infringed.

This trend to build privacy into the planning of applications is most welcome and, in part, I assume it to be a response to the fact that consumers themselves take privacy increasingly seriously and will exercise choice if a particular enterprise is found not to take privacy seriously. Therefore any business which does not take privacy seriously is risking its reputation and, eventually, its bottom line. The fact that citizens themselves are now serving as powerful advocates for privacy reinforces my belief that my Office has a real role to play in educating consumers to ensure that they exercise choice in terms of how they make their information available and to whom.

Challenges posed by new and evolving technologies

One of the key challenges that data protection authorities face is to ensure that data protection continues to be relevant to the medium in which data is being processed. In this respect, it is helpful that data protection legislation applies regardless of the medium, once the data controller is deemed to have a presence in the European Economic Area.

I am often asked what technologies pose the biggest threat to privacy. I tend to prefer not to focus on any one or more technology-specific threat to privacy as technology is evolving so fast. It is clear however, that there is an industry momentum towards the greater use of RFID technology which I highlighted in last year's report. It is clear that such technology poses a great risk to privacy by allowing for the storage and transmission of personal information potentially without reasonable safeguards.

Within the EU these risks have been highlighted by the Article 29 working group of data protection authorities and in this respect the European Commission completed a consultation process in relation to the deployment of RFID technology. The Article 29 Group of EU data protection commissioners has recommended that the default position in relation to RFID tags should be that they be turned to the off position once they leave the shop or factory floor where their intended use has ceased. If it comes to my attention that RFID tags are being used to monitor consumer behaviour, without their knowledge, I will move quickly to ensure that such behaviour is corrected.

SOCIAL NETWORKING

A relatively new phenomenon that came increasingly to the attention of my Office during the course of the year was that of social networking sites such as Bebo, Myspace and Facebook. Bebo, in particular, seemed to attract attention due to both positive and negative media coverage. These sites all have a common feature in that they are hosted outside the EU. I am satisfied that data protection law can be applied to access to material on these sites but, at present, a general movement towards a greater understanding of their responsibilities would lead me to believe that punitive options may not have to be considered in any great detail against such sites.

In considering and discussing these issues, we have to recognise that there is something of a generational issue at play here, as the users of these sites seem far less concerned about the privacy issues arising than, for instance, their parents. This is a point I touched on earlier when highlighting my intended awareness raising efforts. For the users of these sites, the placing of intimate details about themselves in a space where friends and others have access does not seem unusual.

Of course, if a person takes an informed decision in relation to the positives and negatives of placing such material about themselves on these sites, then that is their business. As a privacy advocate, I would wish to be recorded as respecting such decisions. But a number of difficulties arise. One relates to the issue of the capacity of a minor to give consent. This requires consideration of the age and maturity of the individual concerned. A related issue is whether those who place material on these sites always take full account of the potential longer-term consequences. Maybe an individual might be happy at a particular point in their life to have intimate material posted in relation to themselves, but will they be equally content in five or ten years time when applying for jobs if their so-called "Google personality" produced a profile containing such information?

Accordingly, in communicating with users of these sites, we advise them to try to think a little further down the road. This will be a strong message of the communications campaign which my Office will be running during the course of this year targeted at the 12-24 age group. In this respect, I would intend to work closely with the National Council for Technology in Education (NCTE) in terms of the issues arising.

My Office's responsibility relates solely to the data protection issues that arise in relation to these sites. One such issue relates to consent for the processing of personal information. As indicated above, this in turn is related to the age and maturity of the individual concerned. Another issue is the right of an individual to seek blocking of any personal data in relation to them that is incorrect or that was placed on the site without their consent. This might be a picture of a teacher taken in a classroom context without their knowledge or statements that are false. The powers of my Office do not extend to material that is offensive, pornographic or defamatory. However, such abuses actually require the same response on the part of the websites in question: an effective complaints mechanism that is appropriately staffed with trained personnel who can respond quickly to the issues raised. In relation to at least one site (Bebo) the popularity of the site and the amount of content placed on it increased at an exponential pace over the past year. As a result it was unable to deal effectively with complaints within the resources that were allocated to the policing of the site. This is not to say that the site does not care enough about this issue. On the contrary, the company, albeit a little late, has moved in the early part of this year to put in place a more robust complaints handling mechanism to deal with valid concerns.

As with any normal business, these sites value their reputation. I am confident that they will continue to work hard to get the balance right between free expression and an appropriate mechanism for dealing with inappropriate material, including in relation to data protection.

Privacy Statements on Websites Update

Any website that collects personal details online, offers online payment facilities or services, or collects 'cookies' is required to have a privacy statement. My Office undertook a follow-up audit on website privacy statements based on an initial audit carried out in 2005.

The 2005 audit surveyed 248 government, publicly-funded or grant-aided websites. Overall, 132 websites were identified as not having privacy statements.

We revisited the 132 websites in December 2006. 14 sites that are collecting personal information via feedback / 'contact us' forms are still not displaying privacy statements on their websites. I have requested these organisations to place a privacy statement on their websites and liaison between them and this Office is ongoing.

Codes of Practice

I have previously underlined the desirability of developing a standards-based approach to data

protection across the public, private and voluntary sectors. The development of Codes of Practice with sectors is one means of achieving this aim and is provided for in section 13 of the Acts. Such codes, whether it is ultimately decided to give them statutory effect or not, tailor data protection principles to the particular conditions applying in individual sectors. This helps to clarify for the participants in a sector what data protection means in practice for them. We have seen many instances in the past year where such specific knowledge and increased awareness of responsibilities in a sector would have proven helpful. In addition, the ready availability of a code gives greater transparency to how personal data is used and ensures that a data subject can be fully aware of any relevant issues.

As reported elsewhere in this report, 2006 saw the approval of the statutorily-prescribed 'Health Repayment Scheme Code of Practice' under the terms of the Health (Repayment) Scheme Act 2006. Preliminary discussions have taken place with the Personal Injuries Assessment Board (PIAB) on the development of a code that would in particular clarify the permitted usage of medical reports submitted in support of claims. My Office is also engaging with the National Recruitment Federation and the Irish Insurance Federation with regard to codes of practice for the recruitment and insurance sectors respectively. I will be encouraging more sectoral bodies to develop such codes of practice.

GARDA CODE OF PRACTICE

A particular priority is the development of a Code with An Garda Síochána. A number of meetings were held with Garda management in the course of the year to discuss aspects of the code. A draft of the code was ready for submission to me at end year.

The code is an important initiative by An Garda Síochána to promote a best practice approach to data protection throughout the force. The sensitive nature of the personal information held by our police force makes it particularly important that the highest standards of data protection are maintained. I look forward to being in a position in 2007 to approve the final text of the Code.

International Functions

Cross-border flows of personal data are an increasingly significant phenomenon. The protection of personal data within the EU is governed by a common framework, set out primarily in the Data Protection Directive (95/46/EC). Outside the EU, the position varies widely. The open nature of the Irish economy, and the flows of data associated with this fact, means that we have a particular interest in efforts to develop international data protection arrangements.

ARTICLE 29 WORKING PARTY

The primary method of co-ordination amongst the EU data protection authorities is the Article 29 Working Party on which each authority is represented at commissioner level. It also includes colleagues from the EEA countries, the European Data Protection Supervisor and the European Commission. In this forum the data protection authorities work together to seek to be fully effective in making their voices heard. The work of the group in this past year has continued on many fronts including, for the first time, a joint enforcement action in relation to the health insurance sector.

In the past year we as an Office have placed a particular focus on increasing our contribution to the work of the Article 29 Working Party. We have formally joined and sought to influence the thinking of sub-groups dealing with the sensitive issue of the treatment of medical data and the challenges posed by developing technology. Our objective is to ensure that the outcomes of discussions take full account of our views and are therefore easier for us to explain and implement domestically. I would intend that our contribution to this work will increase systematically over time to ensure that we can both influence and be influenced in our domestic focus by discussions at EU level. I accept that it is resource intensive for a relatively small office but I am more than satisfied that the effort, in terms of the impact on the privacy landscape here, will be rewarded.

The Article 29 subgroup on medical data has been active on the preparation of an opinion paper on the use of Electronic Health Records (EHRs). The focus of the draft opinion is on the provisions of Article 8 of the Data Protection Directive and their relevance as a basis for the processing of personal information in EHRs. It is a timely development for the work of my Office, as there has been an increase in queries received in relation to the development of pilot projects in this area. The draft opinion also attempts to provide advice in respect of the development of a national electronic health record system. The finalisation of the opinion in 2007, following consultation with relevant interests, will provide a useful reference point for any system developed in this country.

SWIFT CONTROVERSY

It emerged from US media reports in mid-year that the US Treasury had been accessing details of international financial transfers as part of its efforts to combat the financing of terrorism. The access had been achieved via SWIFT, a Belgium-based company that provides the messaging infrastructure for international financial transfers between financial institutions.

The US Treasury had served subpoenas on SWIFT's US operating centre. SWIFT had decided not to challenge the subpoenas. Neither had it informed financial institutions (including Irish institutions) or data protection authorities that it had granted access to the international financial transactions of their customers. It had, however, negotiated some safeguards with the US authorities.

The actions of SWIFT raised significant data protection issues for EU and other data protection authorities. In its Opinion WP128 of the 22nd November, the Article 29 Working Party concluded that SWIFT and the financial institutions using its services were in breach of their obligations under EU and national data protection law.

I issued a public statement on 24th November welcoming the Article 29 Opinion. The statement continued:

"The Opinion is an important restatement of the principle that actions taken to combat terrorism and serious crime must be proportionate and respect the individual's right to data privacy. My Office will be discussing with Irish financial institutions the action they should take to bring the system they use for international financial transfers into conformity with data protection law".

The representative bodies for Irish financial institutions said that they had been unaware that the US authorities had been given access by SWIFT to their customers' personal information and shared my concern that this had been allowed to happen. They said that they intended to put pressure on SWIFT to take the action necessary to bring its activities into compliance with EU and national data protection law.

Contacts to achieve a satisfactory outcome continued at end-year and indeed into the early part of 2007.

PASSENGER NAME RECORD (PNR)

Another issue which attracted considerable media attention during the course of the year was the Passenger Name Record (PNR) agreement with the US. This provides for the transfer of passenger data from airline reservation systems to the US immigration authorities, subject to agreed safeguards. A revised agreement was put in place during the year, following the striking down of the original agreement by the European Court of Justice (ECJ) at the end of May. Negotiations for a new agreement are due to take place in 2007.

INTERNATIONAL DATA TRANSFERS - BINDING

CORPORATE RULES

Section 11 of the Data Protection Acts outlines the circumstances under which personal information may be transferred out of the State and outside of the European Economic Area (EEA). Regular queries continue to be received in relation to Section 11. Many of these queries relate to the formal instruments which need to be in place before personal information can be lawfully exported.

Binding Corporate Rules (BCRs) are a method of facilitating such international transfers in the interests of business. BCRs allow the composite legal entities of a corporation (or conglomerate) with a separate legal presence in a number of Member States to jointly sign up to common standards for the handling of personal data. This avoids the need for individual contracts between each entity. I am aware that the BCR mechanism has rightly, in the past, received criticism for being slow and cumbersome to progress and therefore unattractive to many companies. For this reason I am supportive of any initiative to bring more clarity to the use of this important instrument for international data transfers insofar as it provides a sound and comprehensive legal basis for such transfers.

THIRD PILLAR GROUPS

While the formal advisory role of the Article 29 Working Party is limited to the First Community Pillar of the EU, my Office also has formal responsibilities in relation to the Third (police and judicial cooperation in criminal matters) Pillar. The Office attends regular meetings in Brussels of third pillar groups - the Europol Joint Supervisory Body and the Customs Information System Joint Supervisory Authority. These groups monitor the data protection issues arising from the activities of Europol and the (relatively low) usage of the customs system. At national level, the Office has responsibility for monitoring the Garda Síochána and customs service use of these systems. The Office also has further duties in relation to the Joint Supervisory Body for Eurojust (co-operation by judicial and prosecution authorities).

SCHENGEN

The Office acts as an observer on the Schengen Joint Supervisory Authority pending Ireland's implementation of the Schengen Information System. This system, together with the systems mentioned above, involves the maintenance of large databases with sensitive personal information, and therefore data protection safeguards are needed.

EURODAC

I am also the supervisory authority in the State for the Eurodac system which is a means of sharing fingerprint data in relation to asylum seekers among member states. The intention is that immigration authorities will be able to readily identify persons who have applied for asylum in another member state or whose application has been rejected by another member state. Eurodac is also subject to the overall supervision of the European Data Protection Supervisor.

As reported elsewhere in this report, my Office carried out audits of the above systems, with the exception of Schengen which is not operational here, during 2006 to ensure that Irish usage of the systems met the highest standards and I am pleased to note that this was the case.

PRUM TREATY

This Treaty, entered into by seven EU member states (Belgium, Germany, Spain, France, Luxembourg, Netherlands and Austria), has the stated aim to help the signatories improve information-sharing for the purpose of preventing and combating terrorism, cross-border crime and illegal migration. There is no indication that Ireland will join the system any time soon but there is a concern that this could be another example of the creation of additional databases, perceived as the answer to security and crime problems, without sufficient justification for the curtailment of privacy that this involves. My Office has participated in meetings with other data protection authorities in relation to the appropriate standards of data protection that need to be in place for its operation.

PRINCIPLE OF AVAILABILITY & DATA PROTECTION IN THE THIRD PILLAR

Within the EU Council, work has also been proceeding in relation to framework decisions on the principle of the availability of information between law enforcement authorities in each Member State and, as a counterbalance, the extension of data protection requirements to all activities in the police and judicial areas. We understand that work on these draft decisions has been rather slow of late.

CO-OPERATION WITH OTHER DATA PROTECTION AUTHORITIES

Continued co-operation with other data protection authorities to ensure the upholding of the data protection rights of citizens does not begin and end with meetings in Brussels. Our close co-operation with our UK colleagues continued, in particular with the Office in Belfast. In the course of the year, there were exchanges of visits with the data protection authorities of Gibraltar and Romania. The Office also benefited from visits from colleagues from the data protection authorities of Italy, Sweden, France and Austria who helped with the training of our new staff. I am most grateful to my colleagues in these data protection authorities for giving so generously of their time.

OTHER INTERNATIONAL MEETINGS

As outlined in my foreword, my colleague the UK Information Commissioner, Richard Thomas, hosted the annual international data protection conference focusing on a single issue: "The Surveillance Society". It proved enormously successful. For a data protection event it attracted a remarkable amount of media attention in the UK. The conference also served to galvanise data protection authorities to take this issue more seriously and go forward in a co-ordinated manner.

My Office also participated in the Berlin Working Group on Telecommunications which brings together data protection authorities and private sector interests from around the world to consider the challenges posed by emerging technologies, including the internet, in the sector.

We also participated in the annual informal gathering of data protection authorities from European common-law jurisdictions which took place in the Isle of Man.

OECD

The OECD has also been advancing work to improve co-operation amongst data protection authorities in tackling privacy breaches which cross boundaries. There are many examples of this, the most obvious being the blight of email SPAM. The Office has only been able to participate in OECD work in a limited way. A particular value of the OECD forum is that it includes non-EU countries of major significance to Ireland such as the USA.

Administration

REGISTRATION ON-LINE FACILITY

In 2006 the number of organisations registered with my Office increased by 447 or 7% (see appendix 2). The Health and Insurance sectors contributed most to the increase.

My Office introduced an on-line registration and payment scheme in mid-November that allows organisations to register or renew their registration via our website, www.dataprotection.ie. Up to year end we had received over 200 applications via this facility. We will be enhancing the features of this facility in 2007 in order to further simplify the registration process.

RUNNING COSTS

The costs of running the Office in 2006 were as follows:

	2005 (€)	2006 (€)	% change
Overall Running Costs	1,391,782	1,281,521	-8%
Receipts	573,421	586,817	+2%

A fuller account of income and expenditure in 2006 is provided in Appendix 3.

STAFFING

The full authorised complement of staff for the Office is 22. At the end of the year we had a full complement of staff.

Part 2 - Case Studies

1. Talk Talk: Unsolicited direct marketing calls
2. Gaelic Telecom / Global Windows: Cold calling
3. DELL: Persistent direct marketing
4. SKY Ireland: Direct marketing by mail
5. Opera Telecom: Forced to delete database
6. News of the World: Limits of Media Exemption
7. Local Authority: Use of PPS Numbers
8. Local Authority: Minutes of council meetings
9. An Garda Síochána: Failure to respond to an access request on time
10. Caredoc: Failure to comply with an access request and appeal of an enforcement notice
11. Barcode/Westwood Club: Failure to comply with an access request for CCTV footage
12. Ashbury Taverns: Failure to comply with an access request
13. Irish Insurance Federation: Complaint about information on central registry
14. School Archiving Project: Disclosure of personal data
15. Ulster Bank: Excessive information sought from new customers

Case Study One

Talk Talk: Unsolicited direct marketing calls

The marketing activity of a telecommunications service provider caused a number of complaints to be made to my Office in the first half of the year. Talk Talk (previously known as Tele 2 which was taken over by Carphone Warehouse and re-branded Talk Talk) was making marketing phone calls to individuals who had already expressly told Talk Talk that they did not wish to be contacted, or who had exercised their right to be recorded on the National Directory Database opt-out register.

Such marketing is contrary to Regulation 13 (4) (a) and 13 (4) (b) of Statutory Instrument 535 of 2003, which states

> *A person shall not use, or cause to be used, any publicly available electronic communications service to make an unsolicited telephone call for the purpose of direct marketing to the line of a subscriber, where-*
>
> *(a) the subscriber has notified the person that the subscriber does not consent to the receipt of such a call on his, her or its line; or*
>
> *(b) subject to paragraph 5, the relevant information referred to in Regulation 14(3) is recorded in respect of the line in the National Directory Database.*

A failure to comply with Regulation 13 (4) (a) or 13 (4) (b) is an offence for which the offender can face prosecution by this Office and direction by ComReg.

In conjunction with ComReg I carried out an investigation of the circumstances which had caused these calls to be made. Given the relatively large number of complaints received in a short period, Talk Talk and its parent the Carphone Warehouse were summoned to a joint meeting with ComReg and ourselves to allow for fuller discussion of the failures which had occurred. This confirmed a clear and unacceptable systems failure in the way in which an agent company of Talk Talk prepared the details of persons to be called.

Given that this was Talk Talk's first offence (albeit a number of offences were committed at the same time), it was decided to give them one opportunity to take remedial action and to put new practices and procedures in place as an alternative to prosecution. In the meantime, Talk Talk undertook to suspend all telesales activity in this country pending the implementation of corrective measures. It was also agreed that, prior to the re-commencement of telesales activity, Talk Talk would make a public apology.

These commitments were honoured and I am glad to say that my Office has not found Talk Talk to be subsequently in breach of its obligations to persons who have expressed a preference not to be called.

This case has highlighted the sanctions available to my Office and ComReg but also demonstrates my overall policy of not moving immediately to prosecution in situations where it is an entity's first offence.

Case Study Two

Gaelic Telecom / Global Windows: Cold calling

I received a number of complaints from the public last year concerning unsolicited calls from Gaelic Telecom, a telecommunications service provider. Of particular concern to me was the fact that many of the complainants were telephoned by Gaelic Telecom even though their preference not to receive direct marketing calls had been recorded on the National Directory Database opt-out register.

My Office contacted Gaelic Telecom in relation to the complaints received. We were informed by the company that, prior to the telephone calls being made, the complainants had received a letter on behalf of their local GAA club asking them to accept a call from Gaelic Telecom. The letter offered them an 'opt-out' which, if responded to, would have removed their number from the database and thereby ensured that no call was made. The company also explained that it sourced details of telephone subscribers on behalf of GAA clubs from club lists, member lists, supporter lists and publicly available databases for the local parish. In some instances, it sourced details through a third-party provider of address lists. Gaelic Telecom provided my Office with a sample copy of a typical letter which issued to telephone subscribers under the name of a local GAA club. The letter offered reduced call charges, discounted line rental and broadband. The local GAA club was guaranteed 15% of call charges incurred by the subscriber every month.

I was particularly disappointed to find that, for the first four months of 2006, Gaelic Telecom had not been checking its direct marketing database against the National Directory Database opt-out register (the register was put in place in 2005). In fact when first approached by my office on this point it didn't seem to even be aware of the existence of the NDD and the requirement to ensure that the numbers phoned were not on the NDD opt-out register.

Over a number of months, my Office adopted a proactive approach to this issue and engaged in intensive communications with the company concerning the complaints received and the remedial measures required. These communications included two meetings with company representatives. We advised them that where the GAA clubs provided lists of members who had given explicit consent to receive marketing calls from Gaelic Telecom, there was no need to check such lists against the NDD. At our request we were provided with revised procedures designed to address shortcomings in their systems. We also asked the company to consider, as a matter of good customer practice, placing an advertisement in the national newspapers to apologise to the public for making unsolicited calls. The company chose not to follow this advice but offered to apologise individually to those who had complained.

As a result of the complaints from the public and my Office's subsequent investigation, I am pleased to report that we have received no further complaints of substance against Gaelic Telecom to date. This demonstrates the important role of the general public in alerting my Office to cases of non-compliance. In this case, complaints from members of the public about Gaelic Telecom's unacceptable practices prevented unlawful direct marketing of other individuals. While I was satisfied with the overall outcome of the case, I was disappointed that Gaelic Telecom did not publicly apologise for their actions. This reflects a somewhat dismissive attitude to the privacy rights of those people whose preference not to receive direct marketing was infringed.

I received a number of complaints last year concerning direct marketing telephone calls made by Global Windows to people whose names had been recorded on the NDD opt-out register. On investigating this matter, my Office found that

Global Windows had been purchasing marketing lists from a third party but the company was not checking the names on those lists against the names on the NDD opt-out register. In response to my Office's intervention, the company suspended marketing operations until it reviewed and improved its internal procedures. Following its review, Global Windows contracted to purchase the NDD opt-out register and it installed a new computer programme to enable it to check its marketing databases against the opt-out register. Despite its efforts to become compliant with the requirements of the data protection legislation, I was disappointed to find that one of the company's telemarketing agents subsequently used an old database to phone a number of people, including a person who had previously complained to my Office. This was a most unsatisfactory development and it demonstrated the critical importance of deleting out-of-date databases. Global Windows acknowledged its error and immediately deleted all old databases to ensure there was no recurrence. Marketers must comply with the requirements of the data protection legislation. In that regard, it is essential that they check their marketing lists against the NDD opt-out register on a fortnightly basis to ensure that the wishes of people recorded on that register are respected. The use of out-of-date marketing lists is an unacceptable practice that is likely to result in a marketer committing an offence.

Case Study Three

DELL: Persistent direct marketing

If you do not want to receive direct marketing, you have a right to notify the sender that you object to receiving such material. This request must be made in writing and an organisation that fails to respect your stated preference shall be in contravention of the Acts.

During the course of the year, I received a proportionally large number of complaints from individuals who were continuing to receive marketing material from DELL despite having requested the company to cease sending such material. I viewed this matter particularly seriously as my Office had previously received assurances from DELL (in June 2006) that measures had been put in place to prevent this happening. To be fair to the company, I believe that it was its understanding, at the time that the initial assurance was given, that this was the case.

However, individuals continued to receive marketing material despite having followed the procedures outlined on the back of DELL's mailed brochures to request that such mail be suppressed. Indeed, one of the complainants to my Office in November 2006 had previously complained to me about this matter and, in that case, my Office had received assurances from DELL in April 2006 that she would receive no more marketing material by post.

In view of the seriousness of the situation, a meeting was arranged with DELL representatives in November 2006 at which it was explained to them by my Office that their mailing suppression systems were simply not working. My Office outlined to DELL the unacceptable nature of these continuous breaches of the Acts. The company outlined a serious of system failures that were put forward as explanations for each breach of the Acts that had occurred.

Technical difficulties arising from the utilisation of a complex structure for sending direct marketing material is not an excuse for breaching the Acts and my Office explained to DELL that it would have to take immediate steps to ensure that its mailing lists took account of all requests for suppressions. We warned that failure on DELL's part to rectify the unacceptable position would be dealt with by use of my enforcement powers under the Acts.

DELL cooperated fully with my Office on this issue and has demonstrated a keen desire to resolve the issues that have arisen as soon as possible. The details of the failures also demonstrate the complexity of the marketing efforts that are put in place by major companies who communicate with the public directly. The case also demonstrates that the more links in the chain from the data controller, to the actual issuance of direct marketing, and to the recording of preferences for not receiving such mail, the greater the risk of systems failures occurring which remain the responsibility of the data controller under the Acts.

Case Study Four

SKY Ireland: Direct marketing by mail

I received a complaint from a member of the public in May 2006 concerning a direct marketing communication which he had received from Sky encouraging him to renew his subscription which he had cancelled in 2001. This was the second occasion on which this data subject complained to my Office concerning the receipt of direct marketing material from Sky. In 2005, on foot of the first complaint, my Office had been assured by Sky that the mailing had issued to the data subject as a result of an administrative error and that steps taken to remedy the situation would ensure that it would not occur again. My Office and the data subject accepted Sky's assurances in good faith at that time.

One of the key data protection principles is the obligation on data controllers to retain data for no longer than is necessary for the purpose for which it was collected. In this instance, the data subject terminated his business relationship with Sky in 2001. The company was not entitled to retain the personal data of their former customer and to use it for direct marketing in this way several years later once the person had objected to the receipt of such material in 2005. Retention of personal data for longer than is necessary is a breach of Section 2(1)(c)(iv) of the Acts. Furthermore, as the data subject had previously informed the data controller that he did not wish his data to be processed for the purpose of direct marketing, and as his wishes were not complied with by virtue of the issuing of further direct marketing material in 2006, a breach of Section 2(7) of the Acts also took place.

My Office commenced an investigation and was informed by Sky that the data subject's record had slipped through its data processing procedures. Sky confirmed that the data subject's record had now been properly suppressed, it apologised for the inconvenience caused and it stated that it wished to offer the data subject a gesture of goodwill to address its error.

My investigative powers under the Acts oblige me to attempt to arrange, in the first instance, for the amicable resolution by the parties concerned in a complaint. My Office makes every attempt to achieve an amicable resolution between parties. In this case, Sky's offer of a goodwill gesture was a significant factor in achieving an eventual outcome which was acceptable to both parties. Sky wrote to the data subject, acknowledged that it had sent him unsolicited marketing material, apologised for the inconvenience caused, confirmed that his record had been suppressed and provided television advertising spots to the value of €5,000 to a reputable Irish charity free of charge.

Direct marketing is a commonly used tool which, if applied in a manner which fails to respect the expressed wishes of members of the general public, is an unwanted intrusion and a nuisance. I have strong powers to protect the rights of data subjects in this area and I have no hesitation in enforcing those rights on their behalf. However, this case demonstrates that, where breaches of the Act occur, solutions short of my using my powers are entirely possible and I welcome the innovative approach of Sky in addressing the complaint of the data subject. I am also happy that such gestures have a sufficiently strong impact on the profitability of entities to ensure that appropriate procedures are put in place to minimise the possibility of a re-occurrence of the system failure.

Case Study Five

Opera Telecom: Forced to delete database

I received a complaint from an individual regarding the receipt of an unsolicited text message in November 2005. The message, sent by Opera Telecom, was a promotional message for a subscription service.

When my Office investigated the matter it was discovered that the complainant had attended a major music concert in Croke Park in June 2005. During the concert, those attending were encouraged to text support for the Global Call Against Poverty Campaign. The complainant did so. The information collected from these texts was stored in a database held by Opera Telecom and was subsequently used by the company for the purpose of sending unsolicited direct marketing SMS messages.

In October 2005 Opera Telecom sent a direct marketing text message to the complainant. Regulation 13 of Statutory Instrument 535 of 2003 refers to unsolicited communications, making it an offence in certain circumstances to send direct marketing messages. The message the complainant received was contrary to this Regulation. It also contravened Section 2 of the Data Protection Acts as the personal data in question had not been obtained and processed fairly and was further processed in a manner which was incompatible with the purpose for which it was originally collected.

During our investigation, my Office discovered that 16,000 concert goers had used their mobile phones to text support for the Global Call Against Poverty Campaign. My Office recognised the potential risk of all of these people being subjected to direct marketing in the same way as the complainant had been. Conscious of this risk, I initially requested in a letter to Opera Telecom that they delete the related Database. When it did not comply with this request, I used my powers under Section 10 of the Data Protection Act and issued an Enforcement Notice. An Enforcement Notice is a legal document and it is an offence not to comply with this. Opera Telecom complied with the Enforcement Notice and deleted the database.

This case demonstrates clearly that information collected for one purpose must not be used for another purpose unless the data subject was informed at the time of collection of such an intended use and given an opportunity to object.

Case Study Six

News of the World: Limits of the Media Exemption

Breaches of data protection rights of individuals by publication of material in the media, as described in last year's annual report, remained an issue during 2006. I made two separate decisions in the course of the year that newspapers had breached their obligations under the Data Protection Acts. One such case involved the Sunday World. The other, described below, involved the Irish edition of the News of the World. Both cases involved the publication of information about children of well-known individuals.

I received a complaint on behalf of a data subject, a well-known individual, arising from material published in the News of the World (Irish edition) in 2005. The complaint related to the subject matter of the material published and the manner in which it was obtained. The material published consisted of a photograph of the data subject and child while shopping, together with related text expressly identifying the data subject's child by name and age, and referring to a third party's perception as to how parent and child were getting along. The complainant alleged that consent was neither sought nor obtained prior to the taking of the photograph. The complainant further alleged that consent was not sought nor obtained prior to the publication of the material subsequently in the *News of the World* newspaper. In particular, the complainant alleged that the publication contravened Sections 2(1), 2A (1) and 22 of the Data Protection Acts. The complainant considered that their right to privacy outweighed any purported journalistic purpose or public interest in the publication of their photograph and accompanying text which was the subject of the complaint.

My Office commenced an investigation and wrote to the data controller, News of the World (Ireland). We sought its observations on the alleged contravention of the Acts, in particular in relation to the journalistic exemption contained in Section 22A. This Section provides a "public interest" exemption in respect of the processing of personal data for journalistic purposes. In response the newspaper highlighted that the data subject was a well-known personality who had been the subject of extensive media attention. It claimed that the data subject had, in the past, courted such attention. Given this background, it concluded that there was a public interest in revealing information about the data subject and the parent - child relationship, as illustrated by the photograph and accompanying text. It stated that the information revealed did not constitute sensitive personal data and that, therefore, the conclusion reached by the UK Courts in the case of *Naomi Campbell V. MGN Limited* - cited as the only authority to date dealing with this particular issue - was not relevant to the present case. It concluded that, in the circumstances, "the article amounted to a publication of journalistic material in the public interest….that…fall(s) squarely within the exemption provided by Section 22A of the 1988 and 2003 Acts".

The primary issue to be decided in this case was whether the public interest exemption under section 22A of the Acts in respect of processing of personal data for journalistic etc. purposes applied in respect of the publication of the photograph and text relating to the data subject and child. If the public interest in publication exemption applied, then there would be no breach of the provisions of the Data Protection Acts in this case.

I am obliged by Section 3 of the European Convention on Human Rights Act, 2003, to perform my functions in a manner compatible with the State's obligations under the Convention's provisions. Accordingly, in arriving at my conclusion on the applicability of the Section 22A exemption to the facts of the case, I had regard to the provisions of Articles 8 and 10 of the European Convention on Human Rights and any guidance that the European Court of Human Rights (ECtHR) had provided on how the rights to privacy and freedom of expression should be balanced - the same balance that was at issue in relation to the applicability of Section 22A of the Acts.

In this regard, I noted the Decision of the ECtHR in the case of Von Hannover v. Germany (Application No. 59320/00) - the Princess Caroline case. The Court held that the German courts, in refusing to grant Princess Caroline of Monaco injunctions against newspapers taking and publishing photographs of her, had infringed her rights under Article 8 of the Convention. The photographs in question had shown Princess Caroline engaged in various activities such as shopping, playing sport and at the beach. The Court, noting that the material related exclusively to details of the applicant's private life, considered that "*the publication of the photos and articles in question, of which the sole purpose was to satisfy the curiosity of a particular readership regarding the details of the applicant's private life, cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public.*" In that case, the Court considered that *"anyone, even if they are known to the general public, must be able to enjoy a "legitimate expectation" of protection and of respect for their private life.*"

While data protection law is not specifically dealt with in the Von Hannover Decision, this case was of assistance in helping me to come to a decision as to the appropriate balance between the public interest in freedom of expression and the individual's right to protection of their personal data, as required by Section 22A of the Acts.

Section 22A(3) of the Acts provides that, in evaluating whether a publication would be in the public interest, regard may be had to codes of practice approved by the Data Protection Commissioner pursuant to the Acts. While no such code has been approved, it seemed appropriate, in reaching a determination, to take note of the newspapers' own codes of practice. In making my assessment, I therefore took account of the National Newspapers of Ireland Code of Practice. In relation to children, the Code provides that they should not be identified unless there is a clear public interest in doing so. Relevant factors are identified as the age of the child, whether there is parental permission, and whether there are circumstances that make the story one of public interest, "or, if the person is a public figure or child of a public figure, whether or how the matter relates to his/her public person or office." I also noted that the UK Press Complaints Commission Code of Practice provides that editors must not use the fame of a parent as sole justification for publishing details of a child's private life and that *"in cases involving children under 16, editors must demonstrate an exceptional public interest to over-ride the normally paramount interest of the child"*. I was of the view that these provisions represent a fair expression of how the principles of data protection legislation ought to be applied in relation to children and minors.

In coming to my decision, I also noted the allegation, which was not refuted by the data controller, that the photograph was taken without the consent of the data subject.

I issued a Decision on this case under Section 10(1)(b)(ii) of the Acts. Among other things, I found that it did not appear to me that the public interest claimed by the data controller in publication of the material in question could be such as to justify setting aside the right to respect for a person's private and family life.

I was of the view that the publication of the photograph and text relating to the data subject and child, and the manner of their interaction, could not be justified in terms of the public interest under section 22A. I considered that the material

published breached the entitlements of a child to interact with its parent in a normal way without their relationship being made the subject of public comment through publication in a newspaper.

Having therefore concluded that the journalistic exemptions under section 22A did not apply in this case, I considered whether the processing of personal data involved in the obtaining and publication of the material complied with the other provisions of the Acts, especially sections 2 and 2A thereof. On the basis of my examination, my decision was that the personal data relating to the data subject and child was not obtained or processed fairly, as required under section 2(1) (a) and 2A of the Acts.

This case demonstrates that data protection applies even in relation to the publication of material in the media. However, in such cases, the issue to be considered in the first instance is whether a general public interest could be deemed to apply to the publication of the material. If it does then the general requirements of data protection are set aside. However, if no public interest could legitimately be claimed, then the media must have due regard to their data protection obligations.

Case Study Seven

Local Authority: Use of PPS Numbers

I received a complaint from a member of the public who had submitted an application for planning permission to a local authority on its Rural Housing Application Form. The complainant informed me that she was required to provide her PPS Number on the form and she expressed grave concern that this personal information would become publicly available as the local authority is obliged by law to make planning applications available to the public at its offices during working hours.

Following my Office's intervention on this matter, I am pleased to say that the local authority responded in a positive and quick fashion. It put in place the following measures which were recommended by my Office:

- in relation to all completed Rural Housing Application Forms which were already publicly available in the public counter area, it blacked out the PPS numbers before they were handed over for inspection to any member of the public;
- it blacked out the PPS numbers on all newly received Rural Housing Application Forms prior to their transmission to the public counter area;
- it reviewed its policy on the collection of PPS numbers on the Rural Housing Application Forms following which the forms were altered to exclude the requirement for the provision of PPS numbers in future.

I consider that the requirement to provide personal data in the form of a PPS number for a rural housing planning application to be excessive data, having regard to Section 2(1)(c)(iii) of the Data Protection Acts which provides that data "shall be adequate, relevant and not excessive" in relation to the purpose for which it is kept. Data controllers must examine whether it is absolutely necessary to harvest such personal data. In this case, following my Office's intervention, the local authority had to examine if the particular application forms could be processed without the provision of the PPS numbers and it considered that they could.Incidentally, on a point of information, it should be noted that it is an offence for any person or body to request or hold a record of a PPS number unless they are permitted by law (the Social Welfare Acts) to do so. ***It is the duty of all bodies to ensure that they are specified in law as being so entitled before they request or hold a record of any person's PPS number.*** (This, of course, is not a matter for my Office to enforce or police).

Case Study Eight

Local Authority: Minutes of council meetings

I received a complaint from a member of the public concerning the publication on a local authority's website of the minutes of the Council's monthly meeting. The complainant informed me that his name and address had appeared in the minutes of the meeting in the context of the sale of lands and properties under the Affordable Housing and Shared Housing Schemes. He expressed concern at the publication of his personal data in this way on a local authority website as well as the ensuing exposure of his personal data on search engines.

My Office contacted the local authority on this matter. We pointed to the important principle outlined in the Annual Report in 2003 that, even where there is legislation providing that information must be made available to the public, this may not always mean that it is appropriate to place such information on a website. On foot of my Office's intervention, the local authority took swift remedial action. It removed the document containing the personal data and edited it in such a way that all names and addresses included on it in respect of the Affordable Housing and Shared Housing Schemes were removed. The local authority also contacted one particular search engine that the complainant was concerned about and sought the deletion of the record from its cache. Finally, the Authority undertook to ensure that the website version of its minutes would, in future, be edited to prevent the disclosure of personal data.

I am grateful to the complainant for bringing this matter to my attention. As a result of his complaint to my Office, the procedures that the local authority put in place following our intervention will have a positive impact on the protection of the privacy rights of many individuals.

Case Study Nine

An Garda Síochána: Failure to respond to an access request on time

I received a complaint in July 2005 that An Garda Síochána had failed to satisfy a data subject's request under Section 4 of the Data Protection Acts for access to his personal data.

My Office commenced an investigation which lasted for a period of some eleven months. We established that An Garda Síochána initially provided the data subject with personal data which it had identified from a search of the PULSE database and of manual files held in the Dublin Metropolitan Region South Central area. The data subject was concerned that the search had been restricted and he requested that all databases and relevant filing systems held by the Gardaí should be searched for his personal data. The Gardaí subsequently informed the data subject that a search of archived files had been conducted and that the personal data which he had sought had been located. They explained that the reason this data had not been located during the initial search was because the file had been archived prior to the introduction of the PULSE system. Over the following months, An Garda Síochána released portions of the personal records to the data subject. As part of my investigation of this complaint, I directed my staff to examine all the records and portions of records initially withheld by the Gardaí, pursuant to the Acts. As a consequence of this examination, and a further voluntary release of records to the data subject in June 2006 by the Gardaí following the provision of advice from my Office, I was satisfied that the data subject had received access pursuant to his rights under the Acts.

The fact remains that it took some twelve months from the initial access request before the data subject achieved his full entitlements under the Acts. Section 4(1)(a) of the Acts provides for a maximum response time of forty days to an access request. In this regard, the Gardaí apologised for the delay which they indicated was due in part to a delay in locating the relevant file in the Garda District in which the data subject resides.

The data subject requested a formal decision from me in relation to his complaint pursuant to Section 10(1)(b) of the Acts. My decision found that An Garda Síochána had, indeed, contravened Section 4(1)(a) of the Acts in respect of the delay in complying with the data subject's access request. In that decision I stated that "*I cannot accept that a delay of this magnitude is acceptable for a body such as the Gardaí which has a responsibility to ensure it fully meets its obligations under the Acts especially given the level of sensitive data that it holds.*" In all other respects, I found that the Gardaí had complied with their obligations under the Acts and that the data subject had obtained his access rights. Finally, I considered that the Gardaí should develop a clear policy on data retention and apply for the necessary authorisation to dispose of records that are no longer necessary for operational Garda purposes.

This case highlights the fact that no data controller can consider itself as not bound by the obligations of the Acts. The right of access is an important and fundamental right which every living individual in this State is entitled to exercise in the expectation that data controllers will comply within the forty day time limit.

Case Study Ten

Caredoc: Failure to comply with an access request and appeal of an enforcement notice

I received a complaint from the parents of a child that Caredoc (a medical facility in Carlow) had failed to comply with an access request under Section 4 of the Acts for access to the child's personal data.

My Office received the complaint in January 2006 and commenced an investigation. We established that the child had attended Caredoc in May 2004 and that the access request was made by the solicitor for the child's family in August 2005. Prior to the complaint being submitted to my Office, Caredoc's solicitors informed the legal representative for the child's family that the access request raised matters of serious importance to their clients and that they wished to be absolutely sure of their position prior to making a formal reply.

During the course of my Office's investigation, we exchanged correspondence on several occasions with Caredoc's solicitors. We posed a number of key questions on the matter, none of which were answered to the satisfaction of my Office. At one point we were advised that the access request had thrown up a serious difficulty with which Caredoc was trying to come to terms. Caredoc's solicitors acknowledged that their client owed statutory obligations on foot of the Data Protection Acts but stated that their client also owed a number of other conflicting obligations which needed to be reconciled properly with all the persons concerned before they were in a position to comply with the access request. In later correspondence, my Office was told that the request had raised a fundamental problem for Caredoc concerning the information gathered by them both physically and electronically and that the opinion of Senior Counsel was required. This was accepted in good faith on the basis that such advice would be forthcoming promptly. In a further letter, Caredoc's solicitors informed my Office that genuine difficulties had arisen as a result of the circumstances thrown up by the access request and that Caredoc was anxious not to have any adverse precedents set in relation to the confidentiality issue as between doctor and patient. Throughout the investigation, my Office continued to remind Caredoc of its obligations to comply with the access request and we advised them that failure to proceed to release the information was a contravention of Section 4(1) of the Acts. At the end of June 2006, having exchanged a large volume of correspondence and with no prospect of the legal advice emerging, my Office gave Caredoc's solicitors a final opportunity to respond to the key questions which we had raised with them. They failed to respond and I subsequently served an Enforcement Notice on Caredoc in July 2006 pursuant to Section 10 of the Acts.

There were a number of reasons for my decision to serve an Enforcement Notice on Caredoc. From the information available to me, I believed that information collected by Caredoc on the date in question likely constituted sensitive personal data within the meaning of the Acts. I believed that Caredoc had not complied with an access request and was, therefore, in contravention of Section 4(1) of the Acts. Furthermore, I believed that, given the passage of time and the continued failure of the data controller or their legal representatives to engage substantively with my Office, an Enforcement Notice was required to ensure compliance.

The Enforcement Notice required Caredoc, within a period of twenty one days, to provide the solicitor of the child's family with the personal data relating to the attendance of the child at Caredoc's facility in Carlow in May 2004. In line with their legal entitlements, pursuant to Section 26 of the Acts, Caredoc appealed to the Circuit Court against the requirement specified in the Enforcement Notice. The appeal was listed for hearing in Carlow Circuit Court in December 2006. At the Court hearing, Caredoc withdrew the appeal and agreed to supply the personal data sought.

I was very satisfied with the outcome of this case. Firstly, it ensured that the patient in question received access to their full medical records. Secondly, the case was significant for my Office as I used my full legislative powers to compel the provision of the records in question when Caredoc had repeatedly delayed in doing so. Thirdly, the case was all the more acute as it related to sensitive medical information which a patient has a right to access except in certain very limited circumstances. Finally, the patient in question was a minor and the access request was made on his behalf by his mother.

This case is a perfect example of the effectiveness of Data Protection legislation as it allows for members of the public, regardless of their status or access to legal advice, to request personal information for a maximum of €6.35 and to receive it. If they do not receive the information they have sought, they can complain to my Office at no cost and we will pursue the matter on their behalf.

Case Study Eleven

Barcode/Westwood Club: Failure to comply with an access request for CCTV footage

I received a complaint from a data subject alleging that Barcode Night Club of WestWood Club in Clontarf did not comply with his access request for CCTV footage in respect of himself, which had been recorded at a specified time in the early hours of a morning in August 2005. The data subject requested footage specifically from the cloakroom inside Barcode Night Club and outside the main gate. He had been involved in an incident inside and outside Barcode Night Club, had his wallet stolen and he was injured as a result.

The data subject made his access request and, in doing so, he referred in his letter to the data controller's obligations under the Acts. He included a reference to my Office's website where the data controller could "see all the details surrounding the Act." After the 40 days had elapsed, during which time his access request had not been complied with, he contacted the manager of Barcode/Westwood Club and she said she would look into it. When he called her again on a later date he was told that Barcode/Westwood Club would not be giving him a copy of any data.

My Office commenced an investigation and wrote to the Manager of Barcode/Westwood Club. In a response received from the solicitor for the Club, my Office was advised that the Club no longer had CCTV footage from the relevant time and that it was not aware, at the time that the access request was made, of its obligations under the Data Protection Acts to provide such footage (if it existed then).

The right of access under the Acts to one's own personal data is a key right and it is the starting point for obtaining control over the use of one's own data. CCTV images which capture an individual are personal data relating to that individual within the meaning of the Acts. The Acts define "personal data" as "*data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller*".

I could not accept the explanation offered on behalf of Barcode/WestWood Club that they were not aware of their obligations under the Acts when they received the data subject's access request. This is especially so as the data subject specifically brought their obligations under the Acts to their attention. The solicitors introduced a question as to whether the data existed at the date of the access request, which was twelve days after the date in respect of which the CCTV footage had been sought. However, they subsequently copied to my Office a document which stated that "CCTV tapes are held for 31 days unless the Gardaí make an official request to download to a master tape." It seemed unlikely to me, therefore, that the data had been deleted at the stage of the access request. This retention policy reflects industry practice which is to retain such footage for 28 days. It is also important to emphasise that pursuant to Section 4(5) of the Acts, the deletion of data is not permissible following receipt of an access request - the Data Controller's obligation is to provide whatever data exists at the time the access request is received.

In March 2006, I issued my Decision on this case under Section 10(1) (b) (ii) of the Acts. I found that the data subject was entitled to a copy of the CCTV footage held by Barcode/WestWood Club in respect of the early hours of the morning concerned in response to his access request. I also found that Barcode/WestWood Club were in contravention of Section 2(1)(c) of the Acts as they failed to keep a copy of the CCTV tape as per their own procedures given to my Office. The specified purpose in this case was for the data subject's access request.

There is an onus on businesses which use CCTV cameras to make themselves aware of their data protection obligations. The eight principles of data protection apply to images of persons captured by such cameras, as they do to all other personal data. In particular, data controllers should be aware of the limited retention period which applies to such personal data as well as the need for transparency and proportionality in the operation of CCTV systems.

Case Study Twelve

Ashbury Taverns: Failure to comply with an access request

My Office received a complaint regarding alleged non-compliance with an access request. This complaint was made by a legal representative on behalf of a data subject formerly employed by Ashbury Taverns of Wexford.

As the access request had not been complied with within the 40 day period, my Office wrote to the data controller. When no response was received, my Office also attempted to make contact on numerous occasions by telephone and by registered post.

As my Office had attempted to investigate this complaint and had been stymied by the failure of the data controller to respond, I decided to issue an Enforcement Notice to Ashbury Taverns. The Enforcement Notice required the data controller to comply with the access request within a period of twenty-one days. During that period, my Office received its first correspondence from Ashbury Taverns by way of a letter from its solicitors. My Office was informed that the access request had not been complied with by Ashbury Taverns because it had likely confused its obligations under the data protection legislation with claims made under employment legislation. The letter also stated that the access request had now been complied with. Upon follow-up communication with the legal representative of the data subject, it was confirmed to my Office that the personal data sought in the access request had been provided.

Once again, this case highlights the scope and strength of my enforcement powers. I intend to use these powers on a routine basis where the right of access to personal data is not granted promptly.

Case Study Thirteen

Irish Insurance Federation - Complaint about information on central registry

My Office received a complaint from an individual regarding the refusal of the Irish Insurance Federation (IIF) to delete information from its central registry. The individual concerned had requested that the Irish Insurance Federation remove the details relating to her from the IIF central registry as she believed the information to be incorrect. Under Section 6 of the Data Protection Acts, 1988 and 2003, an individual can request a data controller, who keeps personal data relating to him/her, to have that data corrected or deleted if the information held is inaccurate.

My Office contacted the IIF, which is the representative body for insurance companies in Ireland. We established that, if an applicant for life assurance is declined or is offered insurance on special terms, then this fact will be noted on the central registry administered by the IIF. The entry in the Registry comprises the first three letters of the applicant's surname, the first five letters of the first name, the date of birth, together with the date and codes for the relevant insurer and the type of policy. The Registry does not contain medical information. (If an applicant is given life assurance without any special conditions he/she would not be entered in the Registry). If an individual applies again for some form of cover, the insurance company to which the individual applies may seek a copy of any medical evidence obtained from the insurer to which the individual had previously applied in order to ensure that it is consistent with the new application. (This is an issue which I am taking up separately with the IIF during discussions on a Code of Practice)

The IIF informed my Office that the information on its central registry in relation to the data subject concerned was correct as a life assurance company had refused her a life assurance policy and the entry on the central registry reflected that fact. In addition, evidence was submitted to my Office to show that the data subject was made aware by the life assurance company at the time of her application for a policy that, in the event that she was declined life assurance or offered it with an increased premium, this information would be shared with the IIF central registry and with other insurance companies as a safeguard against non-disclosure or fraudulent claims. While I might have wished that this information would be more prominently positioned (again an issue that will feature in discussions on the Code of Practice), it was nevertheless provided to the data subject.

Following an investigation of the issues involved in this case, my Office contacted the complainant and explained that the information contained on the IIF central registry was factually correct and that she was not entitled to have the information deleted under Section 6 of the Data Protection Acts, 1988 and 2003.

I am grateful to the complainant for bringing this matter to my attention. In investigating her complaint, my Office became aware of the practice of the sharing of medical reports amongst life assurance companies in cases where cover was declined or offered on special terms. While I can see that this practice serves life assurance companies well as a safeguard against non-disclosure or fraudulent claims, I have to consider it in terms of the disclosure of sensitive personal data in the form of medical reports.

From a data protection perspective, there is a strong argument that the disclosure of medical records should be undertaken only with explicit consent and the applicant for insurance should have a right to withhold their consent but (one would assume) on the basis that it may mean a subsequent application to another company not progressing.

Case Study Fourteen

School Archiving Project: Disclosure of personal data

A former pupil of a national school in Dublin complained to me about a disclosure of personal data through the availability of school registers in Dublin City Libraries and in the National Archives. These registers were indexed as part of the Wheatfield Indexing Project in Wheatfield Prison.

The information contained in school registers, including names, addresses and dates of birth, is personal data within the meaning of the Data Protection Acts.

The Wheatfield Indexing Project involved the archiving of certain Dublin national school registers. It was undertaken by the Irish Prison Service, in partnership with the Dublin City Public Libraries. The aim of the project was to reproduce certain school registers in an electronic format by inputting them into a computer database. The information was then made available to the schools involved and was lodged in "The Dublin and Irish Collection" in Dublin City Libraries at Pearse Street and in the National Archives.

The complainant contacted my Office concerning the disclosure of his personal information in this manner.

On investigation, it was established that neither Dublin City Libraries nor the National Archives had actually made the archives or the indices to these archives available to the general public.

This case highlights, among other things, the vast quantity of personal data which is held in school records and the necessity of treating and handling such data in accordance with the Data Protection Acts (the Acts will apply fully to manual data with effect from October 2007). I also recognise and appreciate the importance and significance of indexing and archiving school material as valuable genealogical, historical and sociological resources. However, such indexing and archiving should be carried out in a manner compatible with an individual's right to privacy. In this case, the information indexed and archived was from the relatively recent past, with some records dating back to as recently as 1981, therefore allowing living individuals to be easily identified from the archived information.

This is a matter that my Office is taking up with the Department of Education & Science to allow for the identification of the appropriate balance between the privacy rights of the individual and the broader public interest in such material being available for research purposes.

Case Study Fifteen

Ulster Bank: Excessive information sought from new customers

In September of last year, it was brought to my attention that a branch of Ulster Bank was requiring new customers to provide, for the purpose of opening new current accounts, a copy of their P60 from the previous year, three recent payslips and bank statements for the previous three months. These documents were sought in addition to identity documents, such as passports and driving licences, which credit institutions are obliged by law to require from new customers for the purpose of preventing money laundering.

My Office contacted Ulster Bank on this matter and engaged in lengthy correspondence with it which continued into the beginning of this year. Section 2(1)(c) of the Data Protection Acts provides that data 'shall be adequate, relevant and not excessive' in relation to the purpose for which it is kept. In my Annual Report 2005, I reported in Case Study 7 on a complaint against another financial institution which had obtained from a customer unnecessary personal data relating to employment and salary on the opening of a savings deposit account. In that case, following the intervention of my Office, the financial institution concerned accepted that the information sought by it was excessive and it immediately introduced revised procedures. The current case concerning Ulster Bank differed somewhat as it involved opening a current account with a laser card facility and not a savings account.

Ulster Bank accepted at an early stage of my Office's investigation that the requesting of P60 information should not have happened. It said that this had occurred in an isolated case and it conveyed its apologies for any misunderstanding and inconvenience. It went on to state that it had spoken to the branch concerned to reiterate standard procedures and it had communicated out to all branches to ensure that any documentation requested from customers remains adequate, relevant and not excessive. It also informed my Office that, as a response, it had introduced an 'appointment card' to be given out to new customers at the appointment enquiry stage so that the customer would know exactly what information/ID to bring with them to their interview. It also changed its policy in relation to income confirmation and it issued guidance to its branches in relation to current accounts with no lending functionality (i.e. ATM card facility only) clarifying that no additional income confirmation or bank statements are required in such cases.

My Office continued to press Ulster Bank on the matter of requesting and then retaining payslips and bank statements for other current accounts. Ulster Bank stated that, for address verification purposes under the Criminal Justice Act 1994, it was obliged to request utility bills or bank statements, in addition to identity documents, and to retain them for five years after the customer relationship ends. It also considered that a current account with either a Laser Card and/or overdraft facility entailed a degree of credit risk and that, in the circumstances, it was appropriate and not inconsistent with the requirements of the Data Protection Acts to request additional documentation such as bank statements and payslips.

My Office was satisfied that Ulster Bank distinguished between current account holders who required nothing more than an ATM card facility and those current account customers who required a credit facility such as a Laser card or overdraft on their account. This allowed Ulster Bank to satisfactorily clarify that those customers who do not require a credit facility will not be asked for additional documentation apart from that needed by law for identity and address verification purposes. In accepting the clarification given on this matter, my Office requested Ulster Bank to make comprehensive information available to potential customers on the different requirements for

different situations. We stated that this information should be communicated on the Bank's website and, in particular, on the 'appointment card' given to new customers.

However, my Office did not accept Ulster Bank's interpretation of its obligations to retain identification and address verification documentation for a period of five years after the customer relationship ends. The factual position is that credit institutions are obliged by the Criminal Justice Act, 1994 to retain documentation obtained for identification purposes only for that period of time. The Guidance Notes for Credit Institutions issued with the approval of the Money Laundering Steering Committee in May 2003 supports this position. In addition, Section 45(iii) of the Guidance Notes pointedly refers to 'requesting sight of original copies' of utility bills, bank statements, etc. for address verification purposes and it makes no provision for 'obtaining,' 'copying' or 'retaining' such documents.

My Office informed Ulster Bank that there is no basis in law for the collection and retention of any documents apart from those required for identification purposes. In the absence of a statutory provision to allow for the obtaining and retaining of personal data such as utility bills, bank statements, social insurance or tax documents, etc. in particular circumstances, organisations who do so are, in effect, breaching Section 2 of the Data Protection Acts.

This case highlights again that all institutions need to satisfy themselves on an ongoing basis that information sought from customers is not excessive for the purpose. In addition, where information is sought, even under a legislative requirement, caution should be exercised as to whether there is an appropriate basis for its continued retention.

Part 3 - Guidance

Guidance

Guidance Note on Mobile Telephone Companies and Local Authority Requests for Customer Data

During 2006 I was concerned to learn that mobile telephone companies were being contacted by local authority litter wardens to seek details of mobile telephone ownership. This arose in the context of litter wardens finding mobile phone top-up receipts that were causing litter. There was also a suggestion that this information was being provided seemingly without question in some cases and without the backing of an enactment or by a rule of law or order of a court. My Office considered this matter and issued the following advice:

Requests made by local authorities for such personal information do not constitute "access requests" as provided for in Section 4 of the Data Protection Acts 1988 & 2003. Local authorities cannot use Section 4 to request personal data from data controllers.

Mobile telephone companies (data controllers) which received these requests from local authorities were, it appeared, considering using Section 8(b) of the Data Protection Acts[3] to allow them to over-ride the restrictions on the processing of personal data and to then furnish the local authorities with the information sought. The provision for disclosure in Section 8(b) is permissive only and it does not place any obligations on these companies to provide local authorities with personal information from their customer databases. This provision also carries the qualifier "in any case in which the application of (data protection) restrictions would be likely to prejudice (preventing, detecting or investigating offences)." Therefore, the exemption does not cover the disclosure of all personal information held by a data controller in all circumstances. It only allows for the disclosure of personal information for the stated purposes and only if not releasing it would be likely to prejudice (that is, significantly harm) any attempt by organisations which have crime prevention or law enforcement functions to prevent crime or to catch a suspect. Furthermore, the Data Protection Acts do not contain any provisions regarding the level of fees which data controllers may charge for such services.

In circumstances where local authorities seek this information in an effort to establish the identity of a person who topped up their phone credit and whose receipt has been disposed of in a manner which contravenes the Litter Act, there is a high risk that a person could be wrongly accused if they did not personally dispose of the receipt or if the receipt was further disposed of by a third party. I would expect mobile telephone companies who provide such personal data to local authorities to satisfy themselves that the provision of the information was proportionate to the alleged offence. In practice, they should treat each request on a case by case basis and not automatically provide the personal information. At a minimum, the data controller must be satisfied that the local authority seeking the information is doing so to prevent or detect a crime or catch or prosecute an offender. The data controller must also consider whether the non-release of the personal information sought would significantly harm any attempt by the local authority to prevent crime or catch a suspect (the risk must be that the investigation may very well be impeded). If they do decide to release personal information to the local authority, the data controller should only release the minimum information necessary for the local authority to do its job. Ultimately, it is up to the data controller whether to release personal information under this exemption. Even if the data controller decides that the exemption applies, they still do not have to release the personal information.

[3] Section 8 (b): (Any restrictions in this Act on the processing of personal data do not apply if the processing is…) required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid.

Guidance Note on the Use of Publicly Available Data for Direct Marketing

Last year my Office was contacted by a number of people who had received direct marketing material by post as a result of the publication of their names and addresses on various lists and registers. The authors of these lists and registers were obliged to make them available to the public under law. For example, the Companies Registration Office must make its Register publicly available. Similarly, planning authorities must publish a weekly list of planning applications and planning decisions. All of these documents contain personal data. Section 1 (4) (b) of the Data Protection Acts provides that the Acts do not apply to personal data consisting of information that the person keeping the data is required by law to make available to the public. A key point here is that the exemption from data protection requirements only relates to the information in the hands of those public bodies that are obliged to make it available. Any other entity seeking to use such information once in the public domain must comply with the standard requirements of data protection.This is a point that my Office needed to highlight on a number of occasions and I am glad to say it was readily accepted in all instances by those entities in receipt of the advice.

As a result of the level of complaints made to my Office on this issue, I was asked to provide guidance on the re-use of personal data contained in publicly available documents. Set out below, as an example, is the text of an information note which I provided as guidance to the Companies Registration Office:

This information note sets out the position of the Office of the Data Protection Commissioner on the re-use of personal data contained in information in the CRO Register which the CRO is obliged by law to make available to the public.

The published information contains "personal data" and each living individual is a "data subject" within the meaning of the Data Protection Acts, 1988 & 2003. Accordingly, the recipients of this information are "data controllers" within the meaning of those Acts. If those data controllers intend to use or further process this personal data in any way, they should be aware of the following Data Protection requirements:

Personal data must be processed fairly. Section 2D (1) (b) of the Data Protection Acts obliges a data controller to ensure, as far as practicable, that the data subject has, is provided with, or has made readily available to him or her, at least the following information not later than the time when the data controller first processes the data or, if disclosure of the data to a third party is envisaged, no later than the time of such disclosure:

- the identity of the data controller
- if he/she has nominated a representative for the purposes of the Act, the identity of the representative
- the purpose(s) for which the data are intended to be processed
- any other information which is necessary to enable processing in respect of the data to be fair to the data subject
- the categories of data concerned
- the name of the original data controller.

The Office of the Data Protection Commissioner considers that it would be reasonable for data controllers to meet these requirements as the information in their possession contains the contact addresses of the data subjects concerned.

In addition, in accordance with Section 2(8) of the Data Protection Acts, a data controller who anticipates that the personal data within the CRO published information, for which they are now the data controller, will be processed for the purposes of direct marketing must offer those persons whose data will be so processed a cost free opportunity to object in advance to receiving direct marketing. This applies both to data controllers who intend to use the personal data for direct marketing potential customers and to data controllers who intend to process the

personal data for distribution to third parties for direct marketing by the third parties.

The Office of the Data Protection Commissioner considers that there is no scope for data controllers to target for direct marketing purposes those individuals whose personal data has come into their possession in this way without first having applied this procedure.

Furthermore, data controllers who may have intentions of processing the personal data by placing it on a website (in any format) should be aware that such processing does not meet any of the conditions set down in Section 2A of the Data Protection Acts (processing of personal data) as there is no consent from the data subjects for such processing of their personal data.

The Office of the Data Protection Commissioner holds a strong position on this matter. The Office cannot envisage any case where the processing of personal data obtained in this way is necessary for the purposes of the legitimate interests pursued by the data controller. Such legitimate interests must be balanced with the fundamental rights and freedoms of the data subjects themselves. The Office considers that this balance is not reflected in the posting of such personal information on a website.

Data Controllers who fail to comply with all of the requirements set out above may be deemed to have breached the Data Protection Acts. Breaches of Data Protection legislation may be reported to, and investigated by, the Data Protection Commissioner. Where the Commissioner forms the opinion that a data controller has contravened or is contravening a provision of the Acts, he may use the enforcement powers conferred on him under the Acts. This includes the power to require a data controller to destroy the database concerned.

Guidance Note on the Use of Electronic Mail for Direct Marketing Purposes

As indicated in the main body of the report, the area of marketing by electronic mail including SMS text messaging is one with which my Office is increasingly being called upon to proactively engage. In this context, my Office issued a detailed guidance note on the use of electronic mail for direct marketing purposes to assist individual subscribers and for persons engaged in direct marketing activity. The guidance note draws upon the legislative framework of the Data Protection Acts, 1988 & 2003, Statutory Instrument 535 of 2003 and previously issued best practice guidelines.

FOR INDIVIDUAL SUBSCRIBERS:

Electronic mail (i.e. a text message, voice message, sound message, image message, multimedia message or email message) for the purpose of direct marketing cannot be sent to you without your prior consent unless it is from someone with whom you have a current customer relationship. The Data Protection Commissioner considers that, in order to comply with the provision of the Data Protection Acts concerning the retention of data for no longer than is necessary, and in line with best practice, a 'current customer relationship' exists only where a business and a customer have engaged in a business transaction within the previous twelve months. The rules for direct marketing using electronic mail are simple:

Marketers may send you electronic mail for direct marketing purposes where:

(i)

- You have given them explicit consent to do so within the last twelve months, **or**

(ii)

- they have obtained your personal contact details in the course of a sale to you of a product or service within the last twelve months, they informed you of their identity, the purpose of collecting your contact details, the persons or categories of persons to whom your personal data may be disclosed and any other information which is necessary so that processing may be fair, **and**
- the direct marketing they are sending is in respect of their similar* products and services only, **and**
- you were given a simple cost-free means of refusing the use of your contact details for direct marketing purposes at the time your details were initially collected, and where you did not initially refuse the use of those details, you are given a similar option at the time of each subsequent communication. *(If you fail to unsubscribe using the cost-free means provided to you by the direct marketer, you will be deemed to have remained opted-in to the receipt of such electronic mail for a twelve month period from the date of issue to you of the most recent marketing electronic mail).*

Marketers may not send you any electronic mail for direct marketing purposes in the following circumstances:

- if you have not given your prior consent to receiving such mail within the last twelve months in accordance with the options set out above;
- if the identity of the sender has been disguised or concealed or a valid address to which you can send an opt-out request has not been provided, and **additionally**, where the electronic mail is an email communication, a valid address at which the sender may be contacted has not been provided;
- if you have joined a club to which you pay a subscription for text, multimedia or email message services, unless the direct marketing is directly related to a similar* product or

service to the subscription club of which you are a member.

If you are receiving electronic marketing messages contrary to these rules, you may complain to the Data Protection Commissioner.

FOR PERSONS ENGAGED IN DIRECT MARKETING ACTIVITY:

Electronic mail (i.e. a text message, voice message, sound message, image message, multimedia message or email message) for the purpose of direct marketing cannot be sent by you to an individual subscriber without their prior consent unless it is to a subscriber with whom you have a *current* customer relationship. The Data Protection Commissioner considers that, in order to comply with the provision of the Data Protection Acts concerning the retention of data for no longer than is necessary, and in line with best practice, a 'current customer relationship' exists only where a business and a customer have engaged in a business transaction within the previous twelve months. The rules for direct marketing using electronic mail are simple:

Marketers may send electronic mail (i.e. a text message, multimedia message or email message) for direct marketing purposes to an individual subscriber where:

(i)

- the subscriber has unambiguously opted-in to receive such mail within the last twelve months, **or**

(ii)

- they have obtained that subscriber's contact details in the course of a sale of a product or service to him/her within the last twelve months, they informed the subscriber of their identity, the purpose of collecting his/her contact details, the persons or categories of persons to whom his/her personal data may be disclosed and any other information which is necessary so that processing may be fair, **and**
- the direct marketing material they are sending is in respect of their similar* products and services only **and**
- the subscriber was given a simple, cost-free means of refusing the use of his/her contact details for marketing purposes at the time those details were initially collected and, where the subscriber did not initially refuse the use of those details, they are given a similar option at the time of each subsequent communication (if the subscriber fails to unsubscribe using the cost-free means provided to them by the direct marketer, they will be deemed to have remained opted-in to the receipt of such electronic mail for a twelve month period from the date of issue to them of the most recent marketing electronic mail).

Marketers may not send electronic mail for direct marketing purposes to an individual subscriber in the following circumstances:

- if the subscriber has not opted-in to receive the electronic mail within the last twelve months in accordance with the options set out above;
- if the identity of the sender has been disguised or concealed or a valid address to which the subscriber can send an opt-out request has not been provided, and **additionally,** where the electronic mail is an email communication, a valid address at which the sender may be contacted has not been provided;
- if the subscriber has joined a club to which he/she pays a subscription for text or multimedia message services, unless the direct marketing material is directly related to a similar* product or service to the subscription club of which that subscriber is a member.

Failure by persons engaged in direct marketing activity to comply with these rules is an offence and summary proceedings may be brought and prosecuted by the Data Protection Commissioner. The sending of each unsolicited communication constitutes a separate offence.

**Similar:* is defined in the Oxford English Dictionary as like, alike, of the same kind, nature or amount, having a resemblance.

The Data Protection Commissioner expects persons engaged in direct marketing activity to pay close attention to the limitations which this definition sets down. It is the Commissioner's view that the term 'similar products' referred to above is strictly limited and that direct marketing undertaken on that basis must not breach those parameters.

Guidance Note on Outsourcing ICT Projects - Hosting of Patient Files in the Health Sector

During the last year there has been an increase in queries to my Office in relation to the provision of hosting services for databases of patient information. From a data protection point of view, hosting services firms are involved in the processing of sensitive health data on behalf of data controllers such as hospitals and GP clinics.

In one such case, my Office advised that section 2C(3) of the Data Protection Acts (which sets out responsibilities for data controllers and data processors in relation to security measures) was an important consideration in the development of any system. We also advised that the company should ensure that it was in compliance with these provisions and that suitable contracts were in place with the relevant data controllers.

We stipulated that a policy on retention periods for the data should also be established and highlighted that even in the event that information needs to be archived for long periods, it may be possible to anonymise it to a certain extent but still allow it to be valid for research purposes.

We asked that where hosting services are being utilised, the employment contract of the employees of the IT company should reflect the duty of confidence regarding data accessed during the course of their activities.

Further considerations arise when hosting of the personal information is outsourced to countries outside the EEA, especially in the case of sensitive information where stringent safeguards need to be put in place before the transfer can take place, if indeed the transfer abroad is deemed completely necessary in a specific case.

The general guidance points above in relation to security considerations and the use of contracts (both domestically and for transfers of information outside of the EEA) may be applied to all sectors that engage in the outsourcing of processing operations involving personal information.

Appendices

Appendix 1

Presentations

During 2006 my Office staff and I gave 34 presentations to the following organisations:

Citizens' Advice
- Comhairle x 5 (Dublin, Kilkenny, Cork, Tullamore, Sligo)
- NCGE

Commercial
- National Recruitment Federation
- Theatre Forum

Educational
- UCC Law Society Annual Conference
- Trinity College

Financial Services
- AIB
- Institute of Chartered Accountants in Ireland

Garda Síochána
- Garda Síochána Training College

Government Agencies
- Department of Finance
- Department of Justice
- National Postcodes Project Board

Health Sector
- Beaumont Hospital Ethics Committee
- The Adelaide & Meath Hospital
- The Academy of Medical Laboratory Sciences
- National Council on Ageing and Older People (NCAOP)
- Medical Research Charities Group

Insurance Sector
- The Insurance Institute of Ireland

International
- International Young Lawyers Association AIJA
- Gibraltar Regulatory Authority
- Privacy Laws & Business/EPON

Legal Sector
- Irish Centre for European Law
- Beauchamps Solicitors employment law briefing

Local Authorities
- Dublin City Council
- Homeless Agency

Mixed Seminars
- Data Protection Forum
- Public Affairs Ireland
- Privacy and Data Protection
- Transatlantic Events Ltd

Voluntary/Charity
- Limerick City Homeless Forum

Appendix 2

Registration Statistics 2004 / 2005 / 2006

		2004	2005	2006
(a)	*Public authorities and other bodies and persons referred to in the Third Schedule*			
	Civil service Departments/Offices	127	147	170
	Local Authorities & VECs	144	160	167
	Health Boards/Public Hospitals	60	60	57
	Commercial State Sponsored Bodies	44	45	40
	Non-Commercial & Regulatory	174	178	170
	Third level	50	56	55
	Sub-total	599	646	659
(b)	*Financial institutions, insurance & assurance organisations, persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts.*			
	Associated Banks	46	45	55
	Non-associated banks	66	72	74
	Building societies	7	7	7
	Insurance & related services	303	342	414
	Credit Union & Friendly Societies	445	440	439
	Credit Reference/Debt Collection	35	41	41
	Direct Marketing	65	69	68
	Sub-total	967	1016	1098
(c)	*Any other data controller who keeps sensitive personal data*			
	Primary & secondary schools	572	622	647
	Miscellaneous commercial	130	176	203
	Private hospitals/health	147	149	155
	Doctors, dentists, health professionals	752	850	926
	Pharmacists	850	867	950
	Political parties & public representatives	156	162	166
	Religious, voluntary & cultural organisations	152	186	213
	Legal Profession	615	629	636
	Sub-total	3374	3641	3896
(d)	*Data processors*	549	603	696
(e)	*Those required under S.I. 2/2001*			
	Telecommunications/Internet Access providers	20	27	31
	TOTAL	**5509**	**5933**	**6380**

Appendix 3

Abstract of Account of Income and Expenditure for the year ended 31 December 2006, for the Office of the Data Protection Commissioner

	2005 (€)	2006(€)
Receipts		
Moneys provided by the Oireachtas	1,392,782	1,281,520.60
Registration Fees	573,421	586,817.00
	1,966,203	**1,868,337.60**
Payments		
Staff Costs	937,691	1,020,822.00
Establishment Costs	250,224	178,182.60
Education and Awareness	144,505	59,822.00
Legal and Professional Fees	46,983	4,695.00
Incidental and Miscellaneous	13,379	17,999.00
	1,391,782	**1,281,520.60**
Payments of Fees to the Vote for the Office of the Minister of Justice, Equality and Law Reform	573,421	586,817.00
	1,966,203	**1,868,337.60**

The financial statements of the Office are subject to audit by the Comptroller and Auditor General and after audit are presented to the Minister for Justice, Equality and Law Reform for presentation to the Oireachtas.